

**C**

ountering Hostile Surveillance

**Detect, Evade, and
Neutralize Physical
Surveillance Threats**

ACM IV Security Services

CONTENTS

INTRODUCTION

PART I

Surveillance and Surveillance

- Countermeasures Overview

Chapter 1

The Hostile Surveillance Threat

Chapter 2

Introduction to Surveillance

- Countermeasures

PART II

Surveillance Operations Techniques

- and Surveillance Countermeasures

- Applications

Chapter 3

Surveillance Operations Overview

Chapter 4

Transition Stages

Chapter 5

Restrictive Terrain

PART III

Surveillance

- Countermeasures Theory

Chapter 6

Surveillance Countermeasures,

- Principles

Chapter 7

Surveillance Countermeasures

- Concepts

Chapter 8

The Chaos Theory of Surveillance

PART IV

Surveillance

-
Countermeasures

-
Applications: Manipulation

Chapter 9

Isolation Overview

Chapter 10

Isolation Methods

Chapter 11

The Break in Contact

PART V

Surveillance Countermeasures

-
Applications: Exploitation

Chapter 12

Introduction to Surveillance

-
Countermeasures Procedures

Chapter 13

The Multiple Sightings Surveillance

-
Detection Procedure

Chapter 14

The Temporary Break in Contact

-
Surveillance Detection Procedure

Chapter 15

The Break and Disappear

-
Antisurveillance Procedure

Chapter 16

The Temporary Break in Contact

-
Antisurveillance Procedure

INTRODUCTION

... For the people resemble a wild beast, which, normally fierce and accustomed to live in the woods, has been brought up, as it were, in a prison and in servitude, and having by accident got its liberty ... easily become the prey of the first who seeks to incarcerate it again ...

—Machiavelli (circa 1515)

Physical Surveillance is the art of hiding in plain sight and stalking an unwitting prey ...
... Surveillance Countermeasures is the art of isolating the stalker and reducing the hunter to the hunted ...

—ACM IV (circa 2006)

The world around us is a dangerous and hostile one. Just as Machiavelli noted, ignorance of the evil makes for easy prey. We have entered an era with a level of prolific predators whom Machiavelli could never have fathomed, even as he penned those prophetic words. We will discuss the hostile threat in greater detail in [Chapter 1](#), but in virtually all cases, the elements that threaten individual, corporate, or national security conduct surveillance operations either to further their objectives or as a primary means to an end.

In today's hazardous environment, security professionals must understand the threat and be able to advise clients regarding the appropriate countermeasures to protect against a hostile surveillance effort. Even the average citizen has security concerns and can benefit from gaining an understanding of the concepts of *surveillance countermeasures* that enhance personal protection.

Surveillance countermeasures are actions taken by an individual or security detail to identify the presence of surveillance, and if necessary, to elude or evade the individual or group conducting the surveillance.¹ In basic terms, surveillance countermeasures are actions taken to identify or evade a surveillance effort. Surveillance countermeasures consist of *surveillance detection* and *antisurveillance*. Although there are many categories of surveillance, this instructional manual focuses specifically on the detection and evasion of *physical surveillance*, which involves an individual or group of individuals moving by foot or vehicle in order to observe and monitor the movement of a target individual.

Over the years, ACM IV Security Services has discovered that the application of surveillance detection and antisurveillance measures is only marginally effective when the individual or security detail does not understand the theory, cause, and effect on which the measures are based. In fact, there is an infinite number of possible surveillance detection and antisurveillance maneuvers, but it is the underlying conceptual basis that makes them effective. The mere application of such techniques is amateurish by design if not planned and executed within the context of how surveillance countermeasures theory applies to surveillance practices. Unfortunately, in many cases, the rote practice of textbook methods without the full appreciation of the “art” and “science” of surveillance detection and antisurveillance measures can lead to costly—and even lethal—consequences.

This manual is unique in scope, as it is certainly not another basic reference on surveillance detection, countersurveillance, and antisurveillance. ² Books and manuals abound with various tried-and-true methods and tactics to detect and evade hostile surveillance efforts. This manual is based on the assumption that the reader has an understanding of, or access to, this readily available information. What is not as readily available or intuitive to the security professional, however, is a reference on the art, science, and theory behind this key aspect of personal protection, given the wide range of potential threats. In fact, it is almost alarming that many security professionals and individuals who regard themselves as security experts are really masters only of the tactics, and not of the theory behind the tactics.

This manual details surveillance countermeasures concepts, techniques, and procedures that are proven effective against the spectrum of surveillance capabilities ranging from the very basic to the world's most sophisticated. This manual does not instruct to the "lowest common denominator," as most tactics-focused publications do. Rather, this manual takes the opposite approach, as the practitioner who can apply techniques and procedures that can defeat the most capable adversaries can certainly defeat the lesser threats. The execution of *techniques* as components of a methodical *procedure* to effectively manipulate and exploit a hostile surveillance effort is representative of a security professional operating at the "Masters" level of surveillance countermeasures tradecraft.

UNDERSTANDING HOW THE SURVEILLANCE THREAT THINKS AND REACTS

This is the basis of effective surveillance countermeasures. The techniques and procedures presented in this manual represent concise applications of the most effective surveillance countermeasures based on a comprehensive analysis of hostile surveillance threats. Understanding how a surveillance effort will perceive and react to these countermeasures is vital to the effective application of specific surveillance countermeasures techniques. Individual surveillance detection and antisurveillance tactics are readily identified as such by a surveillance effort, and overcome. As opposed to a reliance on individual surveillance detection and antisurveillance tactics (maneuvers), this manual presents a process approach that enables systematic, discreet, and comprehensive applications for surveillance countermeasures methodologies.

Surveillance countermeasures applications must be conducted with an appreciation that the surveillance effort they are directed against has a strategy, is proficient, and can react and adapt based on the situation. Actions without perspective are tantamount to those of a chess player who jumps on the opportunity to take a knight with a pawn, without consideration of his opponent's strategy, intentions, and second- and third-order reactions.

Against an able opponent, it is likely that by opting for the immediate tactical success in seizing the knight, the player has contributed to a chain of events that will eventually lead to his demise in checkmate.

Chess analogies aside, the "mean streets" are not sterile environments, and even the most effective surveillance countermeasures tactics may be counterproductive if executed without a well-grounded appreciation of how a surveillance effort thinks and reacts.

Manipulate and Exploit

Manipulation and exploitation are at the heart of the surveillance countermeasures process. They require an understanding of how a surveillance effort thinks and reacts. An appreciation of how a surveillance effort will react to an isolated event is an important perspective, but it is a minimalist approach. The execution of effective surveillance countermeasures is a process. The ability to devise and execute effective surveillance countermeasures *procedures* requires an understanding of the overarching *principles* and *concepts* that translate into surveillance countermeasures tactics, techniques, and methodologies. The key point is that effective surveillance countermeasures procedures are comprised of tactics and techniques that constitute a methodical process. The integration of these common surveillance countermeasures tactics into techniques that *manipulate* and ultimately into procedures to *exploit* a surveillance effort represents the mark of a true professional.

Ingenious in Their Simplicity

This is how the true security professional should view the applications of advanced surveillance countermeasures principles, concepts, techniques, and procedures. Ironically, these sophisticated aspects of art and science are easily understood when they are broken down into their most basic elements. This manual presents intricate concepts in a methodical manner that truly does make them appear simple once broken into their components.

This manual is organized into five parts that must be studied in sequence in order to develop the incremental basis of understanding and to fully appreciate the principles and theory that translate to art, science, and execution. The information herein is presented in a technical and straightforward manner, as the intent is to inform and not to entertain. For this reason, the manual has been specifically designed as a concise reference manual for security professionals that can serve as a relevant framework for the development, training, and execution of security programs.

Reducing the Hunter to the Hunted

This concept is the essence of surveillance countermeasures. Every day and in all parts of the world, hostile surveillance efforts are stalking and exploiting unwitting prey. This manual demonstrates how the intended prey can employ expertise and ingenuity to detect, evade, and if necessary, completely assume the role of the predator in the neutralization of a hostile surveillance threat.

ENDNOTES

1. Surveillance countermeasures terminology is not always consistent among security agencies and professionals. The primary difference is that some use the term *countersurveillance* as synonymous with the term *surveillance countermeasures* used in this manual. Others use the term *countersurveillance* as synonymous with the term *antisurveillance* used in this manual. Although perhaps in a minority (since the term *countersurveillance* has a very specific meaning in the classical sense of espionage

and surveillance in which the firm is actively involved) ACM IV Security Services prefers to use the term *surveillance countermeasures* as the tactics, techniques, and procedures employed to counter the efforts of a hostile surveillance effort. The concepts and applications presented in this manual are consistent, regardless of the reader's preference in discipline terminology.

2. While this manual will address some specific tactical applications, these examples are provided within the context of applicable surveillance detection and antisurveillance principles, concepts, techniques, and procedures. In fact, a detailed discussion of tactical applications would only serve to detract from the primary focus, which is the much more important aspects that enable true security professionals to understand the principles and concepts that drive the formulation and effective employment of tactical applications as part of a coherent process. The book *Surveillance Countermeasures* (ACM IV Security Services) is an excellent reference for specific surveillance countermeasures tactics and techniques.

Surveillance

and

Surveillance

Countermeasures

Overview

The Hostile Surveillance Threat

The new reality of the contemporary environment is characterized by a wide range of unconstrained threats that reflect the ever-growing and pervasive underworld of dangerous actors. The plethora of acute threats to the personal privacy and security of average citizens consist of common criminals and stalkers, private and corporate investigators, government-sponsored espionage agencies, and international crime and terrorist organizations.

In fact, the criminal enterprises that traffic in everything from drugs to human beings, and the terrorist organizations that recognize no bounds of conscience, epitomize the contemporary threats that do not acknowledge innocent bystanders and from whom no one is immune. As a disturbing omen, there is consensus among national security experts that the steady increase in threats to a wider range of individuals based on the disturbing trend of “pervasive insecurity” will continue well into the second quarter of the 21st century.

The spectrum of surveillance threats to personal security can range from surveillance operations with nonlethal intent to the most dangerous extreme: operations conducted in preparation for some type of physical attack.

At the most basic level, criminals will case potential targets to develop information to maximize their probability of success in committing a crime. Although not generally associated with sophisticated surveillance efforts, another common threat to the personal security of many is the stalker threat, which involves surveillance of an individual for any number of reasons—none of which are in the best interests of the target individual. Less sophisticated criminal threats will also employ surveillance to develop information on potential victims for incriminating or exploitable purposes, such as blackmail or coercion.

Criminal, terrorist, espionage, and various other more sophisticated elements employ surveillance to develop information on individuals they intend to intimidate, exploit, or terminate. At the lower end of this threat spectrum, surveillance is employed to develop exploitable information in efforts to recruit or coerce unwitting individuals to provide information or other types of support. Even people with no readily exploitable attributes can be manipulated into compromising situations to develop the leverage necessary for coercion. At the higher end of the lethality spectrum, terrorists, assassins, and other murderous elements conduct comprehensive preoperational surveillance to maximize the probability of successful attacks. In preparation for criminal or terrorist acts, surveillance is employed either to monitor a target’s activity to determine where he is most vulnerable, or in preparation for the conduct of an actual attack.

Another factor that portends an enhanced threat across the spectrum is that the surveillance capabilities that were traditionally associated only with government-sponsored intelligence and security agencies have proliferated widely. Organizations such as criminal, terrorist, and corporate-sponsored elements now have the resources to conduct sophisticated surveillance operations that were previously associated with only the most capable governments. The fact that these elements have training

facilities and doctrinal manuals reflects a degree of sophistication that presents significant challenges to the community of security professionals.

The duration of a surveillance operation depends largely on the sophistication and objectives of the surveillance effort. A surveillance effort to develop information on a target for purposes such as blackmail or coercion will normally be conducted in a more deliberate manner and will generally require more extensive coverage. A surveillance effort to determine when and where a target will be most vulnerable to attack will take relatively less time, because the surveillance effort will focus on key weaknesses rather than on the development of detailed evidence. And in the extreme, a very hasty surveillance effort may be conducted to find and fix the target just prior to an attack. Regardless of circumstances, the target cannot assume that there will be multiple opportunities to detect or evade surveillance, and should in turn exercise diligence at all times.

The objectives and importance of surveillance countermeasures are based on the logical and time-tested assumption that individuals conduct surveillance of a target only in order to do that individual harm. Although the existence of a surveillance effort will always imply some degree of harmful intent, it is the threat of physical harm that most vividly highlights the importance of surveillance countermeasures. Even a random or spontaneous act of crime is preceded by detectable indications. The effective identification of these indications could provide the time and opportunity to react in an evasive manner under life-or-death circumstances. In the case of the more deliberate and sophisticated physical threats such as terrorism, kidnapping, or assassination, the perpetrators will invariably conduct surveillance of the intended victim. In most cases, the surveillance efforts in preparation for these attacks can be readily detected, and in fact, post-event investigations of actual attacks regularly determine that there were detectable signs that the victims overlooked or disregarded due to a lack of security awareness.

SURVEILLANCE TERMINOLOGY

Surveillance is the systematic, discreet monitoring of an individual to develop information regarding his or her activities. Although there are many categories of surveillance—such as technical surveillance—this manual focuses specifically on the detection and evasion of *physical surveillance*. Physical surveillance involves an individual or group of individuals moving by foot or vehicle in order to observe and monitor the movement of a target individual. This is the most challenging and threatening form of surveillance in today's environment.

For purposes of clarity and brevity, the individual under surveillance is referred to as the *target*. The target will also be referred to generically as *he*. The term *target* can refer specifically to the individual, or if under the protection of a security element, the term may refer to the target individual and his security detail collectively. Many surveillance and surveillance countermeasures publications and training courses commonly refer to the target as the *principal*. This manual uses the term *target* because that is exactly what he is when in the crosshairs of a hostile surveillance effort. Despite this distinction, this manual will progressively detail methodologies to facilitate “reducing the hunter to the hunted.” In the final section, we will demonstrate how the target can rapidly transition status from that of a potential prey, to that of the predator.

The element conducting surveillance of the target will be referred to as the *surveillance effort*. A surveillance effort can range from one individual to a sophisticated operation consisting of numerous individuals with specialized vehicles, communications equipment, and other technical equipment. Although a surveillance effort can range from one to multiple personnel, the effort operates with a single focus and will therefore be referred to as *it* rather than “they.”

The physical surveillance methods addressed in this manual are basically categorized as *vehicular surveillance* or *foot surveillance*. The term *surveillance asset* is used to refer to either a surveillance vehicle or foot surveillance operator. When the distinction between vehicle and foot is necessary, the surveillance asset will be specifically referred to as either a surveillance vehicle, or surveillance operator when on foot.

In order to be effective, a surveillance effort must physically observe the target’s activities. For the purposes of this manual, when a surveillance effort is effectively following and observing the target, this will be referred to as maintaining *contact*. The term “in contact” is synonymous with “under observation.”

SURVEILLANCE METHODOLOGY

A professional and effective surveillance effort is orchestrated in a systematic manner, employing tactics and techniques that best ensure discreet coverage of the target. These time-tested procedures are based largely on an understanding of how the average person observes his surroundings while walking or driving.

A surveillance operation will normally begin with limited information regarding the target’s activities. As information is developed during the course of an operation, the surveillance effort will develop a pattern of the target’s standard practices and routines that it will use to plan and conduct subsequent phases of the surveillance operation in a more secure and efficient manner. This process, referred to as *target pattern analysis*, is conducted to determine standard patterns of activity that can serve to effectively focus the surveillance effort.

A surveillance effort generally becomes more efficient and effective against a target after observing his actions over a period of time and becoming more familiar with his activities. This enables the surveillance effort to better anticipate the target’s intentions and actions. This also enables the surveillance effort to determine the times and activities that are likely to satisfy the objectives of the surveillance, as opposed to those that are routine and insignificant. Target pattern analysis enables the surveillance effort to concentrate efforts on the times and events with the highest potential payoff, while limiting the amount of time that it is exposed to the target, risking potential detection or compromise.

The concept of target pattern analysis is a key consideration as it applies to the planning and execution of surveillance countermeasures. Generally, a surveillance effort will adjust its coverage based on how surveillance-conscious the target is observed or perceived to be. If the surveillance effort assumes that the target is not surveillance-conscious based on target pattern analysis and other information and observations, it will likely be less security-conscious in the employment of its tactics and the exposure of its assets. Conversely, if the surveillance effort suspects that the target may be surveillance-conscious, it will exercise greater operational security and will provide the target fewer opportunities for observation and detection.

A driving principle of surveillance is that most surveillance efforts will routinely break contact with a target rather than accept a high risk of exposure. Most surveillance efforts make operational security their highest priority, because if the target becomes aware of coverage, the surveillance effort is severely hindered or rendered completely ineffective. At the conceptual level, this is a key consideration as it applies to the planning and execution of surveillance countermeasures.

Introduction to Surveillance Countermeasures

Surveillance countermeasures consist of surveillance detection and antisurveillance. Although surveillance detection and antisurveillance have two different objectives, many principles and concepts apply equally to both. For the purposes of this manual, the term *surveillance countermeasures* is used when the concepts and applications being addressed apply to both surveillance detection and antisurveillance.

SURVEILLANCE DETECTION OVERVIEW

Surveillance detection consists of efforts taken to detect the presence of surveillance. Such measures consist of actions taken by the target (or a security detail escorting the target) to identify indications of, or to confirm the presence of, a surveillance effort.

Physical surveillance detection can be subcategorized as *passive* or *active*. *Countersurveillance* is a more sophisticated and resource-intensive method of active surveillance detection. Although passive surveillance detection and countersurveillance are important surveillance countermeasures methods, this manual will focus primarily on active surveillance detection measures that are employed by the target, or a security detail escorting the target.

The principles of *observation* are key to surveillance countermeasures, particularly as they apply to surveillance detection. Surveillance is the act of *hiding in plain sight*. This is based on the understanding that the average individual would never suspect that the crippled homeless man, the loving couple, or the ice cream truck could possibly be surveillance assets. Surveillance professionals understand psychological factors such as perceptions and biases, and play on these factors as a form of applied science. The reality is that surveillance assets must maintain a range of vision with the target that is reciprocal. The art of hiding in plain sight lies in the fact that the target will invariably “see” surveillance assets during the course of an operation, but unless he is acutely surveillance-conscious, will not actually perceive them as such.

The effectiveness of all surveillance detection measures depends on the target’s ability to observe his surroundings.

Surveillance detection maneuvers must factor in the ability to observe the desired reaction, because obviously even the best executed surveillance detection maneuver will be ineffective if the target cannot observe for the reaction of a possible surveillance effort.

One of the most effective methods of detecting a surveillance presence is to isolate surveillance assets for observation, retention, and subsequent recognition. However, this method of surveillance detection is time-consuming and assumes that there will be multiple opportunities to detect individual assets over time. This is not always a safe assumption, particularly against a more sophisticated surveillance effort that employs effective tactics, disguise techniques, and even rotates assets. Additionally, the time

required to conduct this deliberate method of surveillance detection is generally longer, and therefore assumes a less immediate threat, which is a risk that many targets and security details are unwilling or unable to accept. As a *procedure*, this method will be addressed in a later section, but not in intricate detail, because this manual is primarily focused on the more proactive and direct *techniques* that cut straight to the determination of whether or not a surveillance effort is present.

Passive Surveillance Detection

Passive surveillance detection consists of the target (or a security detail escorting the target) observing the surroundings to identify indications or instances of surveillance without taking any active measures. A general understanding of surveillance principles and tactics facilitates the effective application of passive physical surveillance detection. In fact, passive observation techniques serve as a basis for hostile surveillance threat awareness. Passive surveillance detection is conducted during the course of normal activities and is primarily based on an understanding of how a surveillance effort operates in order to identify activities or tactics that are indicative of surveillance. Passive detection is conducted in a manner that does not provide the surveillance effort, if present, with any indication that the target is observing for a surveillance presence.

Passive surveillance detection is most feasible when the risk of violent activity against the target is low, making the identification and neutralization of the surveillance threat, if present, less urgent.

Although passive surveillance detection is not usually effective in quickly identifying surveillance, it should always be employed in order to identify indications of surveillance that may justify the employment of more aggressive (active) surveillance detection techniques. In fact, personal security details continuously practice passive surveillance detection as a minimum baseline procedure.

Active Surveillance Detection

Active surveillance detection involves specific, usually preplanned maneuvers to elicit a conspicuous and detectable reaction from a surveillance effort, if one is present. As with passive detection, active surveillance detection is based on an understanding of how a surveillance effort operates. Such an understanding enables the target to employ active measures that will invoke compromising actions by the surveillance effort. In fact, active surveillance detection maneuvers are specifically designed to force surveillance assets to react in a manner that isolates them for detection. By orchestrating an unanticipated situation to which the surveillance effort must react, the target isolates one or more surveillance assets for detection. Active surveillance detection is employed when the target has identified specific indications of surveillance, or as a standard security practice prior to conducting private or protected activities.

The variations of surveillance detection tactics and techniques are virtually infinite, and essentially limited only by the imagination. Although a detailed explanation of surveillance detection maneuvers is beyond the scope of this manual, for perspective, typical examples consist of:

1. Move into a turn lane or an exit ramp and then back into the general flow of traffic, observing for following vehicles that do the same.
2. Cross over multiple lanes of traffic to make a turn or exit and observe for following vehicles that do the same.
3. Drive into a highway exit, such as a rest stop, that enables the target to continue through without stopping, and reenter the highway while observing for following vehicles that do the same. Along city and other streets, there are many variations of this tactic that can be applied, such as through a strip mall or virtually any other parking lot that facilitates a smooth exit and reentry onto the main route.
4. Cut through a parking lot to bypass a red light. This is also an effective antisurveillance measure against a security-conscious surveillance effort.
5. Cul-de-sacs and dead-end streets are probably the most extreme types of restrictive terrain where surveillance assets may be induced into compromising situations by mirroring the target's actions.
6. The 180-degree-turn (reversal of direction) is perhaps the most effective surveillance detection technique. Just as the name implies, this maneuver involves the target reversing direction and retracing the route just traveled. From the surveillance detection standpoint, the 180-degree-turn is intended to isolate potential surveillance assets and elicit a conspicuous reaction. This maneuver enables the target to observe for potential surveillance assets that are forced to bypass the target, to observe for potential assets that hastily and conspicuously move from the route to avoid bypassing the target, and to observe for potential assets that execute a 180-degree-turn where the target did, or at some other location along the route.
7. The "blind turn" or other tactics employing the concept of a "blind spot" are essentially efforts to manipulate a surveillance effort into mirroring the target in a manner that makes it susceptible to surveillance detection. This concept will be addressed in some detail in Part V.

Countersurveillance

Countersurveillance differs significantly from other methods of physical surveillance detection in that it consists of actions taken by a third party (other than the target) to detect the presence of surveillance on the target. Countersurveillance allows the target to travel in a more natural manner, since he—or his security detail—does not have to concentrate on observing for surveillance coverage. Countersurveillance can be conducted by the target's security detail, but is not conducted by the security personnel who are escorting the target. Among the other key advantages is that

countersurveillance assets are able to position themselves in locations that will provide a field of observation that the target would not be able to achieve himself.

Although the focus of this manual is appropriately first-person surveillance countermeasures, countersurveillance is the most sophisticated and effective method of surveillance detection, and is practiced by many professional security, intelligence, and law enforcement agencies. In fact, intelligence operatives use countersurveillance to ensure that their agents are not compromised, and law enforcement agencies employ it to ensure the safety of their undercover operatives during dangerous operations.

Personal and executive security elements can employ the principles of countersurveillance to provide a layer of protection that is equal to that of the most elite agencies. The practice of sending a security detail ahead of the target to conduct forward route reconnaissance can be considered a form of countersurveillance, but this practice is most commonly conducted for the purposes of physical threat identification or neutralization.

Antisurveillance

Antisurveillance consists of actions taken to elude or evade an identified, suspected, or possible hostile surveillance effort. All antisurveillance measures are considered active, in that the target executes an active measure in order to elude or evade a surveillance effort. Although virtually all antisurveillance measures involve efforts to elude or evade, the most extreme antisurveillance objective—*neutralization*—will be specifically addressed in the final section of this manual. Otherwise, unless specifically noted as an application to neutralization, all other references to antisurveillance and surveillance countermeasures as they apply to antisurveillance involve the antisurveillance objectives of eluding and evading a surveillance effort.

Antisurveillance is employed as a standard security practice prior to conducting private or protected activities, or when the target has identified specific indications of surveillance and there is an immediate need to elude or evade. Since surveillance is always possible, antisurveillance can be employed even when there is no specific indication that surveillance is present. In fact, professionals in covert activities, such as espionage agents, invariably employ antisurveillance activities as a standard practice, due to their extreme need to ensure that their operational activities remain unobserved and undetected.

The number of tactical antisurveillance applications is virtually limitless and not within the scope of this manual, but some of the more common examples are turning or exiting a route at the last minute with no warning, or moving into a designated turn lane and then reentering the main flow of traffic at the last possible instance.

Although very overt and aggressive measures—illegal maneuvers that violate traffic laws—are among the most effective antisurveillance techniques. Running red lights, illegal left-hand turns, and illegal U-turns are among the most basic examples of antisurveillance techniques that gain their very effectiveness based on the fact that they are illegal. In many cases, not only will a surveillance effort—in order to maintain security—not continue to pursue the target after such an illegal maneuver, but depending on the nature of the element, they may not want to risk being pulled over by law enforcement for a violation. Covert or illegal elements conducting surveillance

cannot risk that type of exposure. A primary purpose of this manual, however, is to demonstrate that antisurveillance can be accomplished through sophisticated procedures that alleviate the need to carry out isolated, overt measures that will be readily identified as surveillance countermeasures.

As it applies to hostile threats, there is a distinction between antisurveillance and antipursuit. This manual addresses the techniques as they apply to the measures taken to elude a surveillance effort, or even to evade an aggressive effort that attempts to maintain contact despite active surveillance countermeasures. However, if and when a surveillance effort transitions into the attack phase of an operation, the target's efforts should transition as well from an antisurveillance to an antipursuit effort. This manual addresses the spectrum of antisurveillance techniques ranging to aggressive measures to evade determined surveillance efforts. However, antipursuit measures—such as defensive and evasive driving techniques—as they apply to the reaction to the threat of physical attack, are beyond the scope of this manual.

Surveillance

Operations

Techniques and

Surveillance

Countermeasures
Applications

Surveillance Operations Overview

INTRODUCTION

Although this section largely addresses surveillance operations, the specific aspects discussed apply to surveillance countermeasures. The intent, however, is not to provide a detailed reference on surveillance operations. Rather, the purpose is to provide a basic understanding of surveillance operational concepts and techniques as they apply to the examination of subsequent surveillance countermeasures issues. For this reason, it is important to note that essentially every point made here, and in the other two sections in [Part II](#), is relevant to the concepts, techniques, and procedures that are built upon in [Parts III](#), [IV](#), and [V](#). By discussing some details regarding surveillance countermeasures applications up front, the later sections are able to provide more concise explanations of the advanced surveillance countermeasure methodologies.

SURVEILLANCE IMPERATIVES: CONTACT AND MIRRORING

There are two overarching imperatives that any surveillance effort must adhere to in order to execute an effective physical surveillance operation: *maintaining contact* (observation) and *mirroring*. These two simple imperatives are the driving factors for the development and execution of surveillance countermeasures ranging from the most basic to the most sophisticated.

Maintain Contact (Observation)

A surveillance effort must maintain contact with the target through observation in order to ensure that the target is not lost and the surveillance can proceed effectively. Simply stated, if a surveillance effort is unable to maintain contact with the target, the objectives of that particular stage of the surveillance operation will not be achieved. *Although intuitively obvious, this simple fact is the driving concept behind the development and execution of the most effective surveillance countermeasures tactics, techniques, and procedures.*

Mirroring

In a general sense, a surveillance operation involves *mirroring* the actions of the target. Mirroring refers to the tendency of a surveillance effort and individual surveillance assets to duplicate the target's maneuvers. Obviously, it is the requirement to maintain contact that leads to the need to mirror the target's actions. As will be addressed, surveillance efforts with multiple assets will employ tactics that are specifically intended to minimize the level of mirroring, in order to enhance security. In fact, the more professional the surveillance effort, the more proficient it will be in employing surveillance techniques that enable it to discreetly maintain contact, while

maximizing the available cover to blend in with the surroundings and concealment to prevent detection. Regardless of degree of sophistication or number of assets, any surveillance effort must generally mirror the target's overall movements in order to maintain contact.

SURVEILLANCE STAGES

A comprehensive surveillance operation is a tactically complex effort, but for the purposes of this discussion, the dynamics of a physical mobile surveillance will be generalized into two basic stages: the *box* and the *follow*.

The Box

The box stage involves positioning surveillance assets to begin a mobile surveillance operation. This consists of positioning surveillance assets to begin the follow when the target emerges from a fixed location such as a residence or workplace, or when the target stops temporarily during the course of a mobile surveillance follow. The box is based on the systematic positioning of surveillance assets around the area where the static target is located in order to prepare for a mobile surveillance follow when the target begins to move. The techniques of the surveillance box basically consist of the logical coverage of roads or routes by which the target can depart the fixed location. In some cases and based on target pattern analysis, a box may be established around an area which the target may be anticipated to travel through, rather than around the target's known or suspected static location.

The Follow

Once the target begins to travel, the surveillance effort will transition to the follow stage, which involves the transition from static positions in the box stage to a mobile surveillance follow and continues throughout the mobile surveillance of the target while traveling by foot or vehicle. A standard surveillance operation will consist of a succession of transitions between the box and follow stages until the operation is terminated. A given phase of a comprehensive surveillance operation will normally terminate when the target reaches a terminal long-term stay location, such as a residence at night or workplace during the day. In the meantime, the surveillance effort will depart to "cool off" and then return to establish the box when target pattern analysis has indicated that the target can be expected to emerge from the location.

The Mobile Surveillance Follow

Most of a standard surveillance operation's time and effort will be spent during the actual follow phase. For this reason, it is during this phase that the target will have the opportunity to employ the widest range of surveillance countermeasures. The follow phase of a surveillance operation can be conducted either by vehicle or by foot. Obviously, the target's mode of travel will dictate the surveillance asset employed. For our purposes here, the tactics for the mobile surveillance follow will be addressed as they apply primarily to a vehicular surveillance. This is appropriate since most targets' travel is usually conducted by vehicle, and virtually all high-risk personnel

traveling under the protection of a security detachment will be restricted primarily to vehicular travel.

Regardless of how many surveillance assets are employed in an operation, at any given time there will always be at least one asset that maintains observation (contact) of the target. Intermittent losses of contact based on anticipating the target's actions, temporary blind spots, and exchanges between assets are normal. However, a surveillance effort will avoid letting the target go unobserved through options that would allow the target multiple alternative routes of travel, unless the effort were confident of the target's destination based on target pattern analysis or other means.

During the course of a follow, the members of a surveillance effort with multiple assets will *hand off contact* with the target among each other. The most basic example of this *hand-off* process is when the target is traveling along a route and then takes a turn onto another road. In this case, the surveillance asset traveling most closely behind the target will continue straight at the intersection, while another surveillance asset that is further out of observation range will take the turn and establish contact (observation) with the target.

The surveillance follow should consist of a succession of handoffs in order to minimize the amount of time that a single asset is exposed to the target for observation and detection. This is also an effective method of disguising the fact that the surveillance effort is mirroring the target's movements. In virtually all cases, however, there is a varying degree of time—normally seconds—when no asset will have contact with the target as the hand-off is executed.

The *floating box* is a surveillance method that is characteristic of a more sophisticated surveillance effort, as it generally requires multiple assets and a voice communications capability between assets. This method requires a minimum of three assets but is most effectively employed with four or more. Just as the term implies, the floating box involves surveillance assets moving at a pace with the target while traveling along parallel routes for a more secure and effective reaction to a turn in either direction. Given the example of a standard city block in a vehicular surveillance, the floating box would consist of at least one asset traveling behind the target on the same road, while other surveillance vehicles travel along each of the two parallel roads.

A complete floating box formation would also include a *lead* asset, alternatively referred to as a *cheating* asset. In the example of the vehicular street surveillance, the lead vehicle will travel ahead of the target on the same route and can warn the surveillance effort of approaching hazards or options, and can be positioned ahead of the potential obstacles in case the following surveillance assets are held up. In some cases, the lead vehicle could be the asset responsible for contact (observation) with the target at a given time.

Whether surveillance assets travel by foot or vehicle, the terrain and traffic patterns will dictate their following distance. In open terrain, the surveillance effort will generally increase following distance due to the greater range of observation for both the surveillance effort and the target. In denser traffic, the surveillance effort will normally follow more closely to maintain observation and be in the appropriate position at critical points along the surveillance route—primarily at traffic options.

Any sophisticated surveillance effort operates based on an understanding of the principles of observation, and will conform to what should be perceived as the norm with respect to the surrounding environment. A surveillance effort must use *cover* and

concealment to protect its activities from observation by the target. The term *cover* here is used in the classic espionage and investigative sense of *cover* for action, which simply means blending in with the surroundings to appear normal. *Concealment* can consist of a number of possibilities to include physical barriers, but generally, in a surveillance operation the primary method of *cover* and *concealment* for surveillance vehicles is other vehicles, and the primary method for surveillance operators on foot is the surrounding pedestrian traffic.

The Mobile Surveillance Follow—Mirroring

The concept of mirroring warrants specific attention in regard to surveillance countermeasures as it applies to a mobile surveillance operation. In most surveillance operations, the mobile follow stage makes up the large majority of the operation. For this reason, it is primarily during this stage that the surveillance effort will have the most exposure to the target and will consequently be most vulnerable to surveillance detection. Although there are other opportunities to detect or elude surveillance, it is generally during the follow stage that the target will employ the most effective surveillance countermeasures techniques. Mirroring is a key aspect that the target will attempt to detect through passive observation and active detection measures.

The degree to which a surveillance effort can conceal instances of mirroring is primarily based on the degree of training, the number of assets, and the sophistication of the effort. In fact, surveillance efforts employ tactics such as hand-offs, the floating box, and lead assets specifically to minimize the degree of mirroring. As a general rule, the fewer the assets available to the surveillance effort, the more it will be required to directly mirror the target's movements in a manner that is susceptible to detection.

Regardless how many surveillance assets are employed in a given operation, at any time there will always be at least one asset that maintains observation (contact) of the target, and will therefore generally travel at a pace similar to the target's in order to maintain a standard secure following distance. Mirroring is basically an effort to place a surveillance asset in a position that best enables maintaining *contact* and best positions the asset in anticipation of the target's next maneuver.

Normally, mirroring consists of the surveillance vehicle maintaining a standard speed and distance (pacing), and changing lanes or taking turns as the target does. At a very basic level, if the target is traveling on a road with two lanes in each direction and is in the left lane, the surveillance vehicle will tend to position itself in the left lane as well in anticipation of a possible left turn. Alternatively, there will be a tendency to follow in the right lane if this is the target's lane of travel.

Although this form of mirroring (also referred to as *silhouetting*) has its surveillance detection vulnerabilities, it is preferable to the alternative, which is to be out of position when the target takes a turn and have to conspicuously cut across traffic in order to maintain contact. Obviously, other factors—such as the amount of traffic and following distance—will impact positioning, as traveling in a different lane than the target does have some advantages in regard to observation and security, if this can be accomplished in a manner that enables the surveillance asset to react appropriately.

The Mobile Surveillance Follow—The Lost Contact Drill

During the course of a follow, the surveillance effort may lose sight (contact) of the target for any number of reasons. When this occurs, the surveillance effort will take the necessary measures to attempt to regain contact with the target before he reaches a traffic option that would provide multiple possible routes of travel (or escape). If the surveillance effort is unable to reestablish contact prior to the traffic option, it must initiate a *lost contact drill* in an attempt to regain contact. The lost contact drill is a standard surveillance technique that involves the systematic execution of a series of maneuvers to regain observation of the target. This basically involves the immediate prioritization of the target's likely routes of travel from the traffic option.

Even when the surveillance effort is confident of the target's route of travel, it will normally, as a standard precaution, send assets to search along alternative routes of travel to prevent losing the target completely and having to terminate the operation. The effectiveness of this technique is directly based on the number of assets available to search along the alternative routes. For example, if a surveillance effort is forced to initiate a lost contact drill at a standard intersection at which it is assumed that the target's most likely option was to continue straight, then the first asset to the intersection would continue straight in search of the target. The next asset to arrive at the intersection will take the second most likely alternative (left or right), and the third asset will turn to check down the remaining alternative route.

Obviously, in this example, if the surveillance effort is limited to one or two assets, then one or two possible routes of travel would not be searched, potentially limiting the effectiveness of the lost contact drill. If adequate assets are available, additional assets reaching the point of lost contact would reinforce along the possible routes in the same order of priority to provide additional search capability at traffic options further along the respective routes.

As will be addressed in the fifth and final part of this manual, the lost contact drill concept is a key component of the most effective surveillance detection and antisurveillance procedures.

Transition Stages

INTRODUCTION

Transition stages (points) present challenges to the surveillance effort from the standpoint of maintaining contact with the target while avoiding detection.

The primary transition points in a surveillance operation are when the target transitions from a static to mobile status and the surveillance effort transitions from a box to a follow, or when the target transitions from a mobile to a static position and the surveillance effort transitions from the follow to the box.

The transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures. At the most basic level of observation and change detection, an observant target is better able to detect surveillance assets as they transition from a static to mobile status, or from mobile to static status. This, coupled with a basic understanding of how surveillance assets can be expected to position themselves to establish a box and subsequently initiate a follow, is key to detecting surveillance.

Although not transitions associated with the transitions of a surveillance phase, two other transition stages that may occur during the course of the follow are the transition from vehicular surveillance to foot surveillance, and viceversa.

These are also elements of the surveillance follow that present a multitude of surveillance countermeasures opportunities if properly exploited.

Transition Stages—Static to Mobile

The positioning of a surveillance effort for a box involves the logical positioning of surveillance assets to discreetly initiate the follow once the target either travels through or emerges from within the box area. Obviously, the number of surveillance assets available will dictate how the box is established. Depending on the number of assets available, the surveillance effort will prioritize positioning based on the target's most likely routes of departure or transit.

This prioritization process is a key concept because if there are not enough surveillance assets to cover all possible routes, then a corresponding number of routes will not be covered based on the assessment that the target is least likely to take these routes. If there is only one asset, that asset will need to be positioned in a location that will ensure that it can both observe the target when he begins to move and initiate the follow. If the number of surveillance assets available exceeds the number of routes, the surveillance effort may opt to employ a *trigger* asset to alert the effort that the target is moving, and to position other available assets sequentially along the possible routes of departure as reinforcements.

When the target begins to emerge from a location where a surveillance effort would establish a box, if present, he will observe for indications of surveillance. In most cases, this will involve no active measures and will consist of passive surveillance detection.

Observation for change detection purposes is most effective in areas where the target is very familiar with the normal surroundings, such as the neighborhood he lives in. The target will initially observe for vehicles or individuals who are conspicuously placed to act as a potential trigger. Unusually placed trucks, vans, or vehicles with tinted windows are particular indicators. As the target begins to move, he will observe for individuals or vehicles that conspicuously transition from a static to a mobile status. When the target departs the potential box location by vehicle, he will observe for vehicles that are located in likely positions to pull out and assume the follow; focusing primarily on vehicles that pull out behind the target from parallel parking positions or from positions adjacent to the primary route, such as parking lots and side streets. Although the list below is not all-inclusive, when observing for possible surveillance vehicles parked along the route of travel or in adjacent areas, the target will specifically look for vehicles exhibiting some of the following indications of boxing surveillance vehicles:

1. Passengers in vehicles (perhaps even with seatbelts on).
2. Engine running and exhaust emanating.
3. Brake light engaged.
4. Windows clear in inclement weather.
5. Interior vehicle lights on.

Transition Stages—Mobile to Static

This transition involves the target stopping during the course of the follow. It is normally associated with a short-term stop, so in the case of vehicular surveillance, the surveillance effort would likely not transition to a foot surveillance to cover the target during the stop. Therefore, the primary objective for the surveillance effort is to establish a box in preparation for when the target begins to move again.

An example of this transition is when the target pulls into a gas station to refuel. This is a good example of a stop with an opportunity to observe surrounding traffic while conducting a plausible activity (refueling). Regardless of the stop location, it should provide a plausible reason for the stop (cover for action) and the opportunity to observe inconspicuously for surveillance assets.

During this transition, there is an inherent vulnerability to detection as the surveillance assets maneuver based on the target's actions, and may be forced to pass directly by the target's position. This effort to establish a box hastily also presents a window of opportunity for antisurveillance if the target begins to move before the surveillance assets are established in their respective box positions.

Transition Stages —Vehicle to Foot

Unless the surveillance effort anticipates the transition from vehicular surveillance to foot surveillance and prepositions operators on the ground, this transition can be one of the most effective from the surveillance countermeasures perspective. In reaction to this transition, if the surveillance effort has sufficient assets it will deploy foot operators to the ground and then establish a box with surveillance vehicles around the target vehicle location. Due to the nature of a foot surveillance,

with its own unique challenges, the transition from vehicle to foot surveillance is also one of the most effective for antisurveillance purposes.

With a more sophisticated surveillance effort, vehicles may be employed to support the foot surveillance by ferrying operators ahead of the target and relaying communications. As another example, an operator in a stationary vehicle can read a map and give foot operators movement instructions or other information, such as possible hazards that the target and operators may be approaching.

If the surveillance effort loses contact with the target during this transition, the surveillance effort is reduced to conducting random foot searches while waiting for the target to return to his vehicle. In this case, the surveillance effort has a means of reinitiating the surveillance when the target returns to his vehicle, but will not be aware of the target's activities while contact was lost. It is interesting to note that espionage operatives who are confident that surveillance is present will use this technique as a primary means of antisurveillance. By eluding surveillance, the operative is able to conduct his operational activity and then return to his vehicle, which is still under the observation of the surveillance effort.

For a sophisticated surveillance effort with multiple assets to operate by foot or vehicle, the foot-to-vehicle transition is standard and will cause no significant problems. Surveillance efforts with limited assets, however, will encounter significant challenges executing this transition in an effective manner. This will normally require that foot assets move at a faster pace as they anticipate the target's return to his vehicle. This sense of urgency to return to the surveillance vehicles and be in position to assume the vehicular follow presents a profile that is susceptible to surveillance detection. If the surveillance assets are unable to discreetly move faster than the target in returning to the vehicles, the transition presents a risk of lost contact that the target can exploit for surveillance countermeasures.

Restrictive Terrain

RESTRICTIVE TERRAIN INTRODUCTION

The terrain and other environmental factors dictate a large part of how a surveillance effort conducts its follow of the target. Canalized terrain, choke points, and traffic hazards are examples of restrictive terrain types that facilitate surveillance countermeasures. Given the requirement to maintain contact with the target, restrictive terrain will usually force the surveillance effort to assume additional risk of detection in order to ensure that observation of the target is maintained.

Restrictive terrain is employed to isolate potential surveillance assets for surveillance detection purposes, and also to conduct or to posture for the execution of surveillance detection and antisurveillance measures. The key enabling concept of restrictive terrain is that the target will force the surveillance effort into a situation that restricts its freedom of movement, making it vulnerable to surveillance countermeasures.

Although a significant enabler for surveillance countermeasures purposes, restrictive terrain is a true double-edged sword for the target who actually suspects surveillance, but does not know whether the intentions of the surveillance effort are lethal or nonlethal. This is a critical consideration when determining whether to employ these enablers, because in many cases the restrictive terrain that the target can exploit for surveillance countermeasures purposes would likely be the very same restrictive terrain that a hostile element would choose to execute an attack on the target, if that were the intent.

Traffic Hazards

Traffic hazards are areas along a route of travel that can force a surveillance effort to slow down or come to a halt, or areas that provide the target multiple options of travel. Generally, if the target enters a traffic hazard ahead of the surveillance effort, or when not under observation by the surveillance effort, the risk of losing the target is significantly increased. Common traffic hazards include intersections with traffic lights and areas of dense traffic. Such hazards can either cause the surveillance effort to move into close proximity with the target or to lose contact altogether. The surveillance countermeasures implications of traffic hazards are obvious, as they force the surveillance effort into a slow-moving or static position that may be readily observable by the target. Particularly when moving from a relatively open area into an area with traffic hazards, the surveillance effort will tend to push in close to the target to avoid losing contact. Traffic hazards support antisurveillance by serving as obstacles to the surveillance effort as well. For example, the target may be able to clear the traffic hazard and “break away” while the surveillance effort is held up.

A category of traffic hazard that requires additional consideration from the surveillance countermeasures standpoint is *traffic options*. Although very common, a location such as a street intersection that provides the target multiple options of

travel is a traffic hazard, because if the surveillance team does not have contact with the target when he passes through the option, the surveillance effort will be forced to initiate a lost contact drill, not knowing the target's direction of travel from the intersection. Although not necessarily restrictive in the physical sense, traffic options in general do restrict a surveillance effort's freedom of movement, as assets will normally be compelled to reduce following distance when approaching the options in anticipation of the target's possible turn or change of direction.

Choke Points

Choke points are terrain features that generally cause traffic to slow down and concentrate in density. Various examples of choke points include construction zones, toll roads and toll booths, and areas where high-traffic, multiple-lane roads merge into fewer lanes. Choke points provide a number of key enabling characteristics in regard to surveillance countermeasures. For surveillance detection purposes, *choke points* may cause a following surveillance effort to slow down and perhaps push in close to the target, facilitating observation and detection.

As they apply primarily to antisurveillance, choke points can provide a degree of separation between the target and the surveillance effort. For example, when the target, traveling ahead of the surveillance effort, clears the choke point, he will be able to break away from a following surveillance effort.

Canalized Terrain

Canalized terrain consists of areas where freedom of movement is restricted to one primary route. Examples of such terrain are stretches of highway, rural roads, road construction zones where entry and exit are restricted, and roadway bridges or footbridges. The key exploitable concept of canalized terrain is that it provides a surveillance effort with no secure parallel routes or the ability to discreetly turn off of the route once committed onto it. By vehicle, oneway streets provide another dimension to a canalized route that further limits mobility for a following surveillance effort.

For surveillance countermeasures purposes, the exploitation of *canalized terrain* negates the ability for the surveillance effort to execute a secure floating box follow, and forces the surveillance effort to commit all its assets along a single route behind the target. Inducing the entire surveillance effort onto a single canalized route enhances surveillance detection through observable factors such as "convoying," by fanning out at the end of the corridor, or through the execution surveillance detection tactics, the most effective (yet potentially overt) of which is the 180-degree turn or reversal of direction. The exploitation of canalized terrain combined with a traffic hazard, choke point, or other type of obstacle becomes an effective antisurveillance measure.

Intrusion Points

Intrusion points are locations with a single primary point of entry and exit. Basically stated, an intrusion point is a location that forces surveillance assets to either "intrude" upon the target in close proximity or break contact and await the target's

exit from the location. Common intrusion points are dead-end roads and cul-de-sacs by vehicle, and small street-side business establishments by foot.

As it applies to vehicular surveillance, dead-end roads and cul-de-sacs are the extreme in terms of *choke points* because they completely restrict movement once committed. Again, restrictive terrain such as *choke points* will also serve to isolate the target with the surveillance effort, making the target extremely vulnerable to attack if that were the intent of the surveillance effort, or if the effort feels that it must act based on being compromised (“fight-or-flight”).

By foot, intrusion points can be selected that enable the target to observe for potential surveillance operators who choose not to enter but rather linger outside awaiting the target’s exit. Intrusion points with a secondary exit, such as a back door to a business, can be exploited to elude a surveillance effort, but such tactics would be readily perceived as overt antisurveillance measures.

Open Terrain

Just as the term implies, *open terrain* consists of areas where there are no, or relatively few, physical obstacles to obstruct observation for either the target or surveillance effort. Open terrain is restrictive terrain from the standpoint that it negates cover and concealment, and therefore restricts freedom of movement.

By drawing a surveillance effort into an area where there is little vehicular or pedestrian cover and concealment, the target can better isolate and identify the surveillance effort. The obvious risk, however, is that if there is a danger of attack from the surveillance effort the target will have set himself up in a vulnerable position by allowing the effort to isolate him in a secluded area.

Open terrain forces a surveillance effort to make a trade-off between line-of-sight observation and how closely it chooses to maintain contact with the target. For instance, if the surveillance effort chooses close contact over distance, it makes itself immediately vulnerable to detection. Alternatively, the surveillance effort that chooses to distance itself for security purposes makes itself much more vulnerable to antisurveillance.

Restrictive Terrain—Foot Surveillance Applications

Surveillance countermeasures principles and techniques generally apply equally to vehicle and foot surveillance. Given this factor, this manual is primarily focused on surveillance countermeasures applicable to vehicular surveillance because this is how most potential targets will spend the majority of their travel time. Additionally, most targets who travel under the protection of security details will travel only by vehicle when there is even a remote risk of surveillance or attack.

In general, there are some basic noteworthy differentiations among foot and vehicular surveillance. By foot, the target does not have the range of vision that is afforded by a vehicle’s mirrors for surveillance detection, making efforts to observe the surroundings for the presence of surveillance more difficult to conceal, if the target is in fact being observed. This makes it easier for a surveillance effort to identify surveillance detection when a target appears unusually observant of his surroundings.

Another disadvantage to foot travel is that it is generally less canalized. While vehicular surveillance is restricted to established roadways and thoroughfares, foot

surveillance affords more flexibility in travel, as foot surveillance operators can maneuver in many directions with equal speed and security. Another significant disadvantage to surveillance detection on foot is that if there is a risk of attack, the target is not afforded the protection provided by a vehicle, and in most cases, the ability to accelerate away from the threat is much more limited.

On foot, the target can use much the same methodology to exploit canalized terrain and choke points as with vehicular surveillance countermeasures. Canalized terrain may consist of any restricted walkway, street overpasses, bridges, and even elevators or escalators if employed with caution. Canalized terrain may offer the target traveling on foot a natural opportunity to facilitate rear observation, but normally it will be exploited through the incorporation of a 180-degree turn or a stop-and-turn.

Public locations such as department stores, malls, business complexes, and parks are among the places in a foot surveillance operation where operators are most vulnerable to detection. In many circumstances, public locations offer variations of restrictive terrain that provide among the best opportunities for surveillance detection and antisurveillance. In most cases, public locations will force surveillance operators much closer to the target than they would otherwise allow themselves to get.

The basic principles of surveillance in public places are similar to those of choke points and intrusion points, in that they force surveillance operators to concentrate and stagnate. The presence of restrictive boundaries and nonstandard terrain imposes unique constraints and vulnerabilities on surveillance operators. The nonstandard terrain works to the benefit of the target for surveillance detection purposes because it forces the surveillance effort to use special or modified tactics. In essence, public locations force a surveillance effort to rely more on adaptability and resourcefulness than on a standard systematic formula of tactics, rendering surveillance assets more vulnerable.

In most circumstances, people on foot are moving with a purpose or destination. Those who are not are easily isolated from the surrounding populace. This is another key aspect of public locations that can be exploited for surveillance detection purposes. When individuals go into a public location, such as a store, they do so with a purpose. When surveillance operators follow the target into a public location, they must immediately contrive a plausible and natural reason for being in the location (cover for action), leaving them immediately vulnerable to detection if they are not able to adapt. In fact, the target can choose public locations that effectively isolate surveillance operators who enter but are not prepared to adapt to the surroundings. Locations with a standard dress code or in which clientele may be expected to dress in a particular manner or undertake a unique activity are very suitable if employed properly.

It is always important to note that surveillance operators will avoid making eye contact with the target because when this occurs, the asset is considered "burned" and of no further use to the surveillance effort.

This phenomenon results in an almost instinctive or compulsive reflex in close quarters that is highly indicative of surveillance.

Surveillance

Countermeasures
Theory

Surveillance Countermeasures Principles

INTRODUCTION

There are three general surveillance countermeasures principles that directly impact the application of surveillance countermeasures across the spectrum, particularly from the perspective of determining the best means to achieve the desired objectives. Not only are these principles important in the formulation and execution of surveillance countermeasures techniques, it is also vital that security professionals understand these principles, because they can be deceptive if taken out of context.

A detailed discussion of these principles is appropriate for any forum addressing surveillance countermeasures, but for the purposes of this manual, these principles reinforce the need for security professionals to take the application of surveillance countermeasures beyond the mere execution of tactics and techniques and advance to a more sophisticated procedural approach. By way of introduction, these three principles are:

1. Surveillance countermeasures principle: the more active, the more effective.

In general, the more active (overt or aggressive) the surveillance detection or antisurveillance maneuver, the more effective it will be in achieving the desired result.

2. Surveillance countermeasures principle: surveillance detection enables antisurveillance.

Active surveillance detection techniques can be effective antisurveillance techniques.

3. Surveillance countermeasures principle: antisurveillance enables surveillance detection. Antisurveillance techniques can also be very effective in achieving the objectives of surveillance detection.

While these principles are widely accepted among the community of professionals, in many cases, they can focus the applications of surveillance countermeasures in the wrong direction if the broader implications are not fully understood. Key to this understanding is that these principles are focused on the execution and effectiveness of individual maneuvers and techniques. As this discussion will demonstrate, by focusing on the tactics rather than on a process, the target is reduced to executing techniques that must be more active or overt in order to be effective. This implies an increased risk that surveillance countermeasures will be identified by the surveillance effort as such, potentially leading to unintended and dangerous consequences.

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

THE MORE ACTIVE, THE MORE EFFECTIVE

In general, the more active (overt or aggressive) the surveillance detection or antisurveillance maneuver, the more effective it will be in achieving the desired result.

The potentially misleading part of this principle is that it equates “effective” with “good.” This can be misleading in the sense that even if a maneuver is effective in detecting or evading surveillance, if the overall process objective includes ensuring that the surveillance effort does not suspect surveillance countermeasures, then the maneuver is not effective in the broader sense. An appreciation of the *covert-overt spectrum* is necessary to understand that there are varying degrees of “effectiveness” based on the specific surveillance countermeasures objectives.

Active surveillance detection and antisurveillance measures are conducted along the range from *covert* to *overt*—hence the term the *covert-overt spectrum*. Covert surveillance countermeasures are executed discreetly and are intended to detect or elude a surveillance effort without being recognized as active countermeasures. Overt surveillance countermeasures are intended to detect or elude with less or no regard whether the surveillance effort detects them as such. In simple terms, the more covert the measure the less active it is, and the more overt the measure the more active it is.

Generally, the more covert or discreet the surveillance countermeasures technique, the less effective it will be in meeting immediate surveillance countermeasures goals. Conversely, the more overt or active the method the more effective it will be in meeting immediate surveillance countermeasures goals. Consequently, the more overt the method, the more identifiable it will be to a surveillance effort (if present) as surveillance countermeasures.

The covert-overt spectrum is based on the target’s subjective professional judgment regarding the need to execute effective surveillance countermeasures versus the acceptable risk of being observed conducting active or overt measures by the surveillance effort, if present. The determination of where along the spectrum of covert to overt the surveillance countermeasure employed will fall is normally based on an assessment of the risk versus the need to positively confirm or elude surveillance activity. If, at a certain point in time, the benefit gained by executing a successful surveillance detection or antisurveillance maneuver does not outweigh the risk of demonstrating surveillance awareness to the surveillance effort, the target will weigh in favor of more covert techniques. Conversely, if ensuring the execution of a successful surveillance detection or antisurveillance method warrants the risk of an aggressive display of surveillance awareness, then the measure employed will be more overt or active.

Based on this understanding, overt methods are more applicable when the need to detect or evade a potential surveillance effort overrides any considerations regarding the need to remain discreet. However, unless the target has reason to suspect that there is a surveillance effort present with immediate hostile intent, the more sophisticated approach to surveillance countermeasures in most cases is to execute them in a manner that does not disclose that the target is surveillance-conscious. As we will see in the next section, the target has many more options and can exploit many more vulnerabilities against a surveillance effort that does not suspect that the target is surveillance-conscious and is practicing surveillance countermeasures.

Given this perspective, if a surveillance countermeasures technique is intended to be effective while not being detected as such, there is a lower *threshold* for how

active it can be before it fails to achieve the desired effect. Alternatively, if the need to detect or evade a potential surveillance effort overrides any considerations regarding the need to remain discreet, then there is no threshold for how active or overt the surveillance countermeasures technique can be. The threshold that applies to a given target is dependent on the overall objectives of the surveillance countermeasures effort.

One key component of the surveillance countermeasures objective that should never be ambiguous to the target is whether he wants to ensure that countermeasures employed are not detected by a surveillance effort as such, or if he is not concerned that the countermeasures will be identified as such. There is no gray area between these considerations, because the implications and consequences on any future intrigue between the target and the surveillance effort are so diametric.

Therefore, based on varying objectives, the covert-overt spectrum is relative to the desired results. With few exceptions, it will be in the target's best interests, at least initially, that the surveillance effort not suspect that the target is surveillance-conscious or practicing surveillance countermeasures. However, there are circumstances when the need to determine for certain whether surveillance is present overrides these considerations. For example, protective services personnel providing security for a high-risk target may be extremely overt in attempting to detect or evade surveillance.

In the end, it is difficult to gauge how active a given surveillance countermeasure can be before it causes an unintended effect or is altogether counterproductive. Variables such as the size and sophistication of the surveillance effort will also impact where this threshold resides. Regardless, the threshold for where the most active measure the target is willing to risk in order to ensure that the surveillance countermeasure is not detected probably runs from the middle to the low end of the covert-overt spectrum. Since the generally more sophisticated, security-savvy target is more limited in his active surveillance countermeasures options than the unconstrained target, he must employ a more sophisticated process to achieve the desired results, rather than rely on the execution of individual overt techniques.

A final consideration in where along the covert-overt spectrum a surveillance countermeasure should be employed involves the classic fight-or-flight response. As with many factors surrounding the surveillance and countermeasures battle, there are a number of psychological factors that apply just as they do in the most savage expanses of the wild. The fight-or-flight response (also called the "acute stress response") simply means that an animal has two options when faced with danger: it can either face the threat (fight) or it can avoid the threat (flight).

Generally, a surveillance effort will place a higher priority on security than it will on maintaining contact with the target, and will therefore choose flight over fight. However, it is important to understand that in some cases, depending largely on the ultimate intent of the surveillance effort, an overt surveillance countermeasure that is identified as such may force the surveillance effort into the fight mode. Any surveillance effort that continues coverage despite knowing that it has been compromised represents an immediate threat to the target, warranting extreme antisurveillance, antipursuit, and protective measures. The most extreme consequence involves an effort that perceives that it has been compromised and is compelled to react in a high-risk or violent manner, rather than run the risk of not having another opportunity with the target. For example, a surveillance effort that is following a VIP

in order to determine where the target would be most susceptible to attack and kidnapping may react by moving directly into the attack phase of the operation if it observes actions by the target that may indicate that he is attempting to detect or elude surveillance.

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

SURVEILLANCE DETECTION ENABLES ANTISURVEILLANCE

Active surveillance detection techniques can be effective antisurveillance techniques.

This principle is based on the valid premise that most surveillance efforts will want to remain discreet and will therefore terminate contact rather than mirror the target's surveillance detection maneuvers in a readily detectable manner. Therefore, overt surveillance detection methods are also effective antisurveillance methods against a security-conscious surveillance effort. Generally, the more *active* (overt or aggressive) the surveillance detection technique employed, the more likely it will be detectable as such by the surveillance effort, and will force it to either terminate the surveillance or pursue the target despite knowing it is compromised.

Whenever a surveillance detection technique is addressed, this concept should be considered as well in order to determine the antisurveillance implications. Most surveillance efforts make operational security their highest priority, because if the target becomes aware of coverage, the surveillance effort is severely hindered or rendered completely ineffective. Any surveillance effort that places a higher priority on maintaining security than it does maintaining contact with the target will normally terminate the surveillance after observing the target execute a surveillance detection maneuver, rather than risk further compromise. Even the most subtle active surveillance detection maneuvers can "spook" a particularly sensitive surveillance effort. For example, with a highly security-conscious surveillance effort, restrictive terrain may serve as an antisurveillance deterrent in and of itself, by forcing the effort to terminate contact rather than commit assets into a potentially compromising situation.

Consistent with the discussion of the previous principle, the degree to which overt techniques are employed must be tempered by the fact that a point is reached at which the technique is counterproductive from the surveillance detection standpoint, because it will only serve to force the surveillance effort to terminate contact. If the overall objective is to detect surveillance without the surveillance effort knowing that it has been compromised, then an active surveillance detection maneuver that serves an antisurveillance function is counterproductive. In most cases, it will be in the target's best interest that the surveillance effort not terminate contact prior to being confirmed as such. For this reason, the target must effectively regulate where along the covert-overt spectrum the method will fall in order to achieve the acceptable risk/benefit ratio that best meets the objectives.

By way of summation, active surveillance detection techniques can place the surveillance effort in a position that forces it to either terminate the surveillance or risk compromise—making them effective antisurveillance techniques as well. *However, this demonstrates that the intended technique (surveillance detection) has an*

unintended result (antisurveillance). This also demonstrates that surveillance countermeasures that give the surveillance effort the ultimate choice (“terminate contact or risk exposure”) are suboptimal. As will be discussed in the conclusion of the section, what is optimal is the employment of surveillance countermeasures processes that incorporates techniques to *manipulate* and *exploit*, and can be executed in incremental stages that are more effective in achieving the desired results, while not being overtly identifiable as such.

SURVEILLANCE COUNTERMEASURES PRINCIPLE:

ANTISURVEILLANCE ENABLES SURVEILLANCE DETECTION

Antisurveillance techniques can also be very effective in achieving the objectives of surveillance detection.

This principle is based on the fact that a surveillance effort that attempts to maintain contact, despite overt antisurveillance efforts by the target, will readily expose itself to surveillance detection. Generally, antisurveillance techniques are executed in a manner that forces the surveillance effort to terminate contact rather than risk exposure to likely detection. For the most part, antisurveillance techniques gain their effectiveness based on the fact that most surveillance efforts will place a higher priority on maintaining security than they will on maintaining contact with the target. Therefore, overt antisurveillance measures are most effective as long as the surveillance effort is not willing to overtly mirror the target’s antisurveillance measures in order to maintain contact.

Antisurveillance is the most difficult surveillance countermeasure to conduct discreetly because the techniques are generally more aggressive and readily identifiable by a surveillance effort. Again, the more overt or active the antisurveillance maneuver, the more effective it will be in eluding or evading surveillance. However, against a determined and capable surveillance effort, only the very most overt techniques will be singularly effective in evasion.

Additionally, these techniques will not meet the overall objective of most targets, as they will be immediately identified as active antisurveillance efforts. For these reasons, antisurveillance techniques employed in isolation, and not as part of a process, are generally ineffective unless the immediate need to detect or evade a surveillance presence overrides all other objectives. Again, except under extreme circumstances, an effort to achieve immediate results at the expense of the broader objectives is generally the exception and not the rule.

As with the previous principle, this demonstrates that the intended technique (antisurveillance) can lead to an unintended result (surveillance detection). Although there is an obvious surveillance countermeasures benefit to detecting the surveillance effort, in the event that a surveillance effort attempts to maintain contact after the target executes antisurveillance maneuvers, it should indicate either that the surveillance effort is tactically unsound from the operational security perspective, or that it is determined to maintain contact despite compromise.

The latter is an immediate concern, as any surveillance effort that continues coverage despite knowing that they have been compromised represents an imminent threat to the target, warranting extreme antisurveillance, antipursuit, and protective

measures. Aggressive antisurveillance techniques that do not force the surveillance effort to break contact are the very most effective surveillance detection techniques, but in virtually all cases, the most important factor that they confirm is that the target is in immediate danger.

This possible eventuality certainly demonstrates that surveillance countermeasures that give the surveillance effort the ultimate choice (terminate contact or risk exposure) are suboptimal. In this case, the target has given the surveillance effort the choice (or compelled it) to continue with the surveillance or pursuit rather than avoid compromise and detection. By conducting antisurveillance techniques that give the surveillance effort a choice (fight-or-flight), the target has orchestrated a situation that may lead to the most dangerous of unintended consequences.

THE PROCESS APPROACH TO SURVEILLANCE COUNTERMEASURES

The principles addressed in this section provide an opportunity to substantiate the broader issue of executing procedures incorporating appropriate techniques, as opposed to employing isolated techniques as the means to an end. This underscores the true challenge and art of surveillance countermeasures, as the target can never truly “reduce the hunter to the hunted” unless the tables can be turned without the surveillance effort knowing that this has been achieved. The lone exception to this is when the antisurveillance objective is neutralization, which will be addressed in the final section of this manual.

The fact that active or overt techniques are more effective in achieving immediate results does not necessarily make their utilization the most effective surveillance countermeasures strategy. While overt techniques may be effective in achieving immediate goals, they are normally not in the best interests of meeting the longer-term objectives of most targets. If an overt surveillance detection technique fails to detect surveillance but does force the surveillance effort to terminate coverage, the technique was not effective and was very likely counterproductive to the target’s overall objectives. If an overt antisurveillance technique fails to evade a surveillance effort, it was certainly not effective and has likely been counterproductive by either inducing the fight response, or compelling the effort into a pursuit.

Overt surveillance countermeasures that are identified by the surveillance effort as such basically force the surveillance effort to make a choice. Whenever the surveillance effort is provided the opportunity to make a choice, the target has relinquished control of the surveillance countermeasures process to the adversary. Not only has the target shown his hand by demonstrating surveillance consciousness, but he has also given the surveillance effort the choice regarding how the next stage of the confrontation will proceed.

Recalling the chess analogy from the Introduction, this is the classic situation wherein the target may doom himself to eventual “checkmate” by seizing the opportunity for an immediate tactical gain. Whether the intended result of a given surveillance countermeasures technique is surveillance detection or antisurveillance, by allowing the surveillance effort the option, the target will very likely not achieve the intended result.

As a final note, the discussion in this section should not be taken to imply that the execution of active surveillance techniques is not appropriate, because they are essential to the execution of effective surveillance countermeasures processes. The main point is that active surveillance countermeasures techniques should not be employed in isolation as an expedient, except when circumstances dictate that aggressive measures be employed based on immediate security concerns. Rather, active surveillance countermeasures techniques should be employed at the time and place of the target's choosing, and as a component of an integrated process.

Surveillance Countermeasures Concepts

INTRODUCTION

As stated in the introduction to this manual, the methodologies, techniques, and procedures presented herein represent concise applications of the very most effective surveillance countermeasures based on a comprehensive analysis of hostile surveillance threats. To this point, the theory and practice of surveillance operations and surveillance countermeasures have been detailed in order to provide a basis for the guiding concepts of surveillance countermeasures.

Based on the analysis of the art and science of surveillance countermeasures principles within the context of the standard surveillance operations methods, key guiding concepts have been derived that scope the development of the primary and most effective surveillance countermeasures techniques and procedures. This section introduces two key concepts that represent the basic components to this methodical approach to surveillance countermeasures. These concepts establish the cornerstone for virtually all surveillance detection and antisurveillance tactics and techniques, and are summarized as follows:

- 1. Surveillance Countermeasures Concept: Be Inconspicuous**

In most cases, and at least initially, it is to the target's advantage that the surveillance effort not suspect that the target is surveillance-conscious or practicing surveillance countermeasures.

- 2. Surveillance Countermeasures Concept: Target Pattern Analysis**

A surveillance effort conducts target pattern analysis to maximize the efficiency and security of the surveillance operation.

A thorough appreciation of these fundamental concepts is essential to the basic understanding of surveillance countermeasures techniques and procedures, and will be referred to throughout this manual, particularly as they apply to the next level of surveillance countermeasures, which are the more specific surveillance detection and antisurveillance procedures.

Concept Summary

The concepts of *be inconspicuous* and *target pattern analysis* are interrelated as they apply to establishing the conditions for effective surveillance countermeasures. Even if surveillance is suspected, whenever feasible it is best initially to maintain a normal pattern of activities without demonstrating any indication of surveillance consciousness or raising suspicions. In this way, the surveillance effort, if present, is allowed to develop a sense of confidence and security regarding its strategy for

surveillance coverage of the target based on target pattern analysis. This also enables the target to assess his own patterns of activities to understand how any surveillance effort would develop and implement a surveillance strategy.

If indications of surveillance are identified through passive surveillance detection, or otherwise, the target can begin to develop a surveillance countermeasures strategy based on the situation. An appreciation of the surveillance threat's target pattern analysis process will enable the target to determine when and where the most effective surveillance countermeasures can be employed.

SURVEILLANCE COUNTERMEASURES CONCEPT: BE INCONSPICUOUS

In most cases, and at least initially, it is to the target's advantage that the surveillance effort not suspect that the target is surveillance conscious or practicing surveillance detection.

Generally, a surveillance effort will adjust its coverage based on how surveillance-conscious the target is observed or perceived to be. If the surveillance effort assumes that the target is not surveillance-conscious, it will likely be less security-conscious in the employment of tactics and the exposure of assets. This should provide better opportunities for the target to detect surveillance. Conversely, if the surveillance effort suspects that the target may be surveillance-conscious, it will exercise greater operational security and will provide the target fewer opportunities for passive observation.

In most cases, a recognizable effort at surveillance detection or antisurveillance will cause the surveillance effort to adjust its tactics or terminate the surveillance altogether. In either case, the result may be counterproductive in the sense that, even if the surveillance effort is not terminated, it may become more sophisticated and much more difficult to detect. Since a primary objective of surveillance detection is to isolate surveillance assets for observation, retention, and subsequent recognition, the termination or enhancement of surveillance coverage could negate opportunities to confirm surveillance by observing surveillance assets at subsequent times and locations.

A final reason for remaining inconspicuous is that it sends a message to a surveillance effort, if present. Any experienced surveillance effort will be very cognizant of surveillance consciousness on the part of the target, unless surveillance countermeasures are executed in a very subtle and effective manner. Generally, surveillance is conducted against a target in order to develop some type of information. A display of surveillance consciousness on the part of the target will be perceived as an indication that he has something to hide.

A surveillance effort will likely intensify its coverage—and perhaps increase the number of assets—if it perceives that the target does have something to hide, and will generally assume a more secure and cautious posture if it suspects that the target is surveillance-conscious. For this reason, any premature activity by the target that heightens the surveillance effort's sensitivities will be counterproductive, as it will place the effort on alert and make it less susceptible and vulnerable to unexpected surveillance countermeasures techniques and procedures.

Although the target may not have the luxury of "waiting out" a surveillance effort, in many cases the best defense against a surveillance effort is to make it unprofitable.

Regardless of the surveillance effort's motivation and capabilities, it will not indefinitely sustain coverage of a target that does not demonstrate activity of operational interest in support of the objectives of the surveillance operation.

SURVEILLANCE COUNTERMEASURES CONCEPT: TARGET PATTERN ANALYSIS

A surveillance effort conducts target pattern analysis to maximize the efficiency and security of the surveillance.

In an earlier section, we addressed *target pattern analysis* as an element of an effective surveillance operation. This factor becomes a key concept that can be exploited for surveillance countermeasures purposes. Based on target pattern analysis, the surveillance effort will tend to develop a sense of security by relying on established patterns to dictate its coverage strategy. Over time, a surveillance effort may be drawn into a sense of complacency that can be readily exploited at the time and place of the target's choosing. When this sense of security is suddenly disrupted by an unanticipated maneuver on the part of the target, the surveillance effort may be forced to react in a manner that leaves it vulnerable to detection.

The effective application of surveillance countermeasures exploits the surveillance concept of target pattern analysis to develop specific strategies to detect or evade a surveillance effort based on the target's self-examination of established patterns of activity. This process enables the target to determine when and where during his routine travel patterns the surveillance effort may be vulnerable to a surveillance countermeasures maneuver, or series of maneuvers.

Surveillance countermeasures maneuvers that are significantly inconsistent with the established patterns will be readily apparent as such to a surveillance effort. For this reason, the target's appreciation of his own target pattern analysis profile is necessary for the development of surveillance countermeasures procedures that would appear more plausible to the surveillance effort, if present.

The Chaos Theory of Surveillance

INTRODUCTION

A key factor in the effectiveness of surveillance countermeasures is the degree to which the surveillance effort is caught surprised, off-balance, or in a compromising position. Although there are a number of situations that can cause such effects, for instructional purposes, ACM IV Security Services captures many of the intangibles of a surveillance operation and refers to this dynamic as The Chaos Theory of Surveillance. This application epitomizes the concept of manipulation and is among the most effective means of reducing the hunter to the hunted.

In mathematics and physics, Chaos Theory addresses the phenomena of how isolated events can destabilize systems. This theory is commonly referred to as the “ripple effect,” and is probably most popularly associated with the “butterfly effect,” which suggests that the flapping of a butterfly’s wings might cause tiny changes in the atmosphere that ultimately cause a tornado to appear.

A surveillance effort employs a systematic approach that involves common tactics, techniques, and procedures. Whether the surveillance effort is a single person or multiple operators, there is basically a set system of methods that the effort will apply in reaction to the target’s movements. With multiple operators, this systematic approach becomes even more important, because each individual operator needs a good understanding of how all the operators can be expected to react to a given situation. This ability to understand how each operator can be expected to react is what makes surveillance a system. The Chaos Theory of Surveillance, and its destabilizing effects, are as applicable to a surveillance effort as the Chaos Theory of physics is to any other systematic approach.

The psychological and physiological factors of confusion, anxiety, friction, inertia, and momentum apply to any surveillance operation. Ironically, even the majority of individuals categorized as “professional surveillance operators” are actually unaware of the advanced concepts that impact most surveillance operations. Such “professionals” understand that these dynamics occur, but have never conducted a critical analysis of the problem to identify the root causes and corrections. These factors that impact a surveillance operation based on confusion, inaction, or overreaction are addressed as they apply to The Chaos Theory of Surveillance, which, if effectively exploited, is the ultimate manipulation of a surveillance effort for isolation, detection, or evasion purposes.

CHAOS THEORY DISCUSSION

Within the surveillance professionals’ community, surveillance operations are affectionately characterized as *hours of boredom periodically interrupted by moments of chaos*.

This tongue-in-cheek characterization implies that even an unwitting target can cause a noteworthy degree of chaos for a surveillance effort. The hallmark of a professional surveillance effort is its ability to react to and manage chaos. However,

chaos that is deliberately created by a manipulative target can be virtually impossible for even the most capable surveillance efforts to manage. Consistent with the above characterization of a surveillance operation, the target can orchestrate moments of chaos to isolate, manipulate, and exploit surveillance assets—hence the term The Chaos Theory of Surveillance.

The course of a standard surveillance operation generally involves the surveillance effort monitoring and recording the target's mundane day-to-day activities. Particularly in the case of a target that does not demonstrate surveillance awareness or consciousness, the surveillance effort will observe the target's routine activities that will likely remain consistent over the course of days and even weeks. This is where target pattern analysis, whether conducted as a formal process or developed repetitively over a period of time, tends to settle the surveillance effort into a sense of security and in some cases overconfidence. Over time, a surveillance effort may be drawn into a sense of complacency that can be readily exploited at the time and place of the target's choosing. When this sense of security is suddenly disrupted by an unanticipated maneuver on the part of the target, surveillance assets may become isolated and even forced to react in a manner that leaves them vulnerable to detection.

When the target conducts an unanticipated activity that is not consistent with target pattern analysis, the surveillance effort will likely assume that the unusual activity is potentially of very high operational interest, since it deviates from established norm. This professional instinct to ensure that contact is maintained while at the same time reacting to an unanticipated event—if effectively exploited—renders the surveillance effort vulnerable to isolation and detection. As a synergistic effect, the laws of psychology and physics can be exploited to cause a situation that is chaotic for the surveillance effort, yet controlled by the target.

Any number of intangible factors build up over the course of a surveillance operation, but two general categories of factors that develop and can lead to poor execution in the face of uncertainty are referred to as *inertia* and *friction*. These elements, in conjunction with the generation of “momentum,” are factors of vulnerability that the target can manipulate against the surveillance effort.

The inertia of a situation is accentuated by destabilizing factors such as the adrenaline of the moment, fear of losing the target, and a drive to accomplish the objectives. In this context, inertia is action based on a general sense on the part of surveillance assets that there is a need to move and react, but an uncertainty regarding exactly what needs to be done. This movement amid confusion and without sound direction is readily exploitable for surveillance detection and antisurveillance.

There are also factors—such as an anxiety about avoiding compromise and even sleep deprivation—that can tend to generate a destabilizing friction. As a potentially debilitating counterbalance to inertia, friction is inaction or hesitation. This is a tendency of some surveillance assets to err on the side of being overcautious under uncertain circumstances. An interesting point is that, in a given situation, surveillance assets may react differently. This can result in a combination of inertia and friction that causes variations in momentum and negative momentum that can very readily desynchronize and compromise a surveillance effort.

APPLICATIONS OF THE CHAOS THEORY OF SURVEILLANCE

The number of exploitable applications of this theory is infinite, and they will differ based on whether the objective is surveillance detection or antisurveillance. Given this understanding, a basic example provided for illustration purposes involves the target traveling to his workplace. Assuming a surveillance presence, the surveillance effort will have likely performed some target pattern analysis and will be aware of the target's standard route to work. As such, as the target progresses along the route to work, the surveillance effort will assume that it is a routine phase of the surveillance, with the target conforming to his established pattern.

As the target is in the final approach to his work location, he can initiate the Chaos Theory by continuing past the work location (or by deviating just prior to reaching it) when the surveillance effort is relaxed and fully anticipating the conclusion to another standard phase of the operation. This will immediately launch the surveillance effort into a reactive mode when it is probably poorly positioned based on the final preparation for the stop and the fact that it is now faced with uncertainty based on this new and irregular activity. At this point, any number of maneuver options are applicable to further exploit the inertia, friction, and general chaos that such a basic action can cause if properly executed.

As with the number of specific surveillance countermeasures, the possible applications of the Chaos Theory are unlimited. In fact, if not for the serious nature of a potentially hostile surveillance effort, the target could "toy with" a surveillance effort using various chaos-inducing methods. Transition points such as temporary stops, transitions from vehicular to foot surveillance, and transitions from foot to vehicular surveillance also provide abundant opportunities to orchestrate chaos scenarios.

The combination of Chaos Theory dynamics with concepts and techniques to be addressed in subsequent sections, such as the "temporary break in contact," "avoid lost contact, and "lost contact reaction" are indicative of a security professional operating at the "master's" level of the trade.

There is no professional surveillance operator with street-level experience who would dispute that such a Chaos Theory exists. Virtually no "professionals," however, have ever examined the phenomenon in detail to understand the alpha and omega of this dynamic, though all have experienced it. This stands as another example of the higher level of understanding needed to master the art and science of surveillance countermeasures. Once again, tactical applications are standard fare, but an understanding of advanced concepts such as The Chaos Theory of Surveillance enables the target to enter, manipulate, and disrupt the hostile surveillance threat's decision cycle and operational process.

Surveillance

Countermeasures

Applications:
Manipulation

Isolation Overview

INTRODUCTION

Isolation is an incremental process that is best characterized as a methodical effort to distinguish potential surveillance assets from the surrounding environs for observation and subsequent *exploitation* as appropriate. The importance of isolating surveillance assets can not be overstated—it is the critical path to effective surveillance countermeasures. The term “isolation” has connotations that could imply a method of “entrapment,” but this is actually the most extreme case. Despite this caveat, the methods of isolation do in a sense transition the target’s role from the “hunted” to the “hunter.”

With very few exceptions, isolation is a prerequisite for effective surveillance countermeasures. Isolation is first and foremost a method of manipulation in support of surveillance countermeasures. The most effective surveillance countermeasures procedures consist of a manipulation stage and an exploitation stage. The manipulation stage is an incremental process of isolation techniques. The isolation process ranges from the initial isolation efforts to identify specific indications of a surveillance presence to the more focused techniques intended to isolate specific surveillance assets in preparation for exploitation. The closing isolation techniques for the most effective surveillance countermeasures procedures generally consist of the target inducing the surveillance asset into a situation or position making it vulnerable to a directed exploitation measure.

The techniques employed to isolate surveillance assets are similar for surveillance detection and antisurveillance, but the combination of techniques employed in a given procedure may vary. Although surveillance countermeasures procedures can be executed in a deliberate manner over hours, the execution of most procedures can be measured in minutes, and in many cases, seconds. This demonstrates that a well-developed and well-executed surveillance countermeasures procedure will efficiently employ a succession of isolation techniques leading to the decisive isolation technique that establishes the conditions for a definitive exploitation effort.

Once potential surveillance assets have been isolated, and depending on the surveillance countermeasures objective, the target can then execute a specific isolation technique as part of a surveillance detection procedure to enable the definitive confirmation of surveillance, or as the basis for manipulation in the initial stage of an antisurveillance procedure. Coincidentally, as we will see in Part V, the most effective manipulation techniques in support of both procedures are the same.

Isolation is a means to achieving detection, but it is not synonymous with detection. Surveillance detection is achieved either by multiple sightings of surveillance assets or by observing for conspicuous actions or reactions that indicate or confirm a surveillance presence. In either case, this requires that potential surveillance assets be isolated for scrutiny and testing. Recall that for any surveillance detection maneuver to be effective, the target must be able to observe the reaction to the maneuver. By first isolating the potential assets, the target can then focus his observation to ensure the detection of surveillance.

The initial isolation technique is invariably based on the surveillance imperative of *maintaining contact*. The incremental process then progresses from the general to the more specific through a succession of mutually built-upon techniques. For example, if the target is traveling down a multilane road, he can essentially isolate potential surveillance assets by observing the general grouping of following vehicles in the positions that a surveillance asset might occupy if present. The general isolation of a grouping of potential surveillance assets would be the initial isolation technique to focus follow-on isolation techniques.

Although in many cases isolation and detection is a progression toward antisurveillance, there are circumstances in which isolation can be much less precise and complete for antisurveillance than is necessary for surveillance detection. Although the degree of isolation depicted in the previous example is certainly not rigid enough for definitive surveillance detection, just the appreciation of where the potential following surveillance assets might be is a sufficient degree of isolation if antisurveillance is employed as a standard security practice, even with no specific indications of a surveillance presence. Granted, most sophisticated antisurveillance efforts would require a greater degree of isolation as a precondition, but this is not always the case.

Isolation Methods

Isolation is a primary component of the manipulation stages of the most effective surveillance countermeasures procedures. Isolation techniques are initially executed to identify potential surveillance assets, and then as the final form of manipulation in order to exploit for definitive surveillance detection and antisurveillance purposes. As they apply to surveillance countermeasures, isolation techniques have three distinct isolation purposes:

1. Isolation techniques to identify potential surveillance assets.
2. Isolation techniques employed as an element of a surveillance detection procedure to detect or confirm a surveillance presence.
3. Isolation techniques employed as an element of an antisurveillance procedure to evade or elude a surveillance presence.

The *isolation purpose* to identify potential surveillance assets (1) is the precursor and the basis for follow-on isolation techniques in support of the most effective surveillance detection (2) and antisurveillance (3) procedures. As it applies to isolation purpose objective (3) above, a section of [Part V](#) (“The Break and Disappear Antisurveillance Procedure”) will pull it all together into the definitive antisurveillance procedure.

As they apply to surveillance detection, once potential surveillance assets are isolated, the most effective procedures to exploit the potential assets involve using one or a combination of the following *exploitation methods*:

1. Observe for retention and later comparison, or to compare with previously identified suspected assets.
2. Elicit a compromising response.
3. Execute a surveillance detection maneuver, or series of maneuvers, to elicit a compromising response.

Exploitation method (1) above (observe for retention and later comparison, or to compare with previously identified suspected assets) is a standard surveillance awareness practice and can stand as a key component of a surveillance detection procedure that will be discussed further in [Part V](#) (“The Temporary Break in Contact Surveillance Detection Procedure”).

Exploitation methods (2) and (3) apply to isolation purpose (2) above. The amalgam of these aspects form the manipulate-to-exploit transition in the definitive surveillance detection procedure, which will be detailed in [Part V](#) (“The Temporary Break in Contact Surveillance Detection Procedure”).

ISOLATION TECHNIQUES INTRODUCTION

This section addresses the techniques that are employed to isolate potential surveillance assets and is a logical continuation of the isolation methodology

addressed in the previous section. Effective surveillance detection requires that potential surveillance assets be isolated for detection. There are three primary categories of techniques through which surveillance assets are isolated:

1. The detection of indications of mirroring. Techniques designed for this purpose are based on the fact that in order to be effective, a surveillance effort must employ the two basic imperatives of maintaining contact and mirroring.
2. The exploitation of restrictive terrain based on an understanding of how restrictive terrain impacts freedom of movement and how a surveillance effort will react to compensate. Techniques designed for this purpose are based on the fact that the exploitation of restrictive terrain is an effective means of isolating a surveillance effort for surveillance countermeasures purposes.
3. The exploitation of transition stages based on an understanding of how a surveillance effort operates in reaction to these stages and the inherent vulnerabilities to isolation. Techniques designed for this purpose are based on the fact that the transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures.

While the concepts behind these three techniques will be discussed in detail, recall that [Part II](#) addressed the imperatives of contact and mirroring, transition stages, and restrictive terrain with applications to surveillance countermeasures. To avoid repetition, readers should refer to [Part II](#) as necessary to augment the information provided as it applies specifically to isolation.

ISOLATION TECHNIQUES CONCEPT OVERVIEW

The imperatives of maintaining contact and mirroring are key guiding concepts for surveillance countermeasures. The irony is that these are such simple concepts, but they are the ones on which the advantage turns to either the “hunter” or the “hunted.” The reality is that the imperatives of maintaining contact and mirroring are significant constraints under which the surveillance effort must operate in order to succeed. In fact, the only way that a surveillance effort can succeed under these conditions is if the target is unaware and its efforts go undetected. With a surveillance-conscious target, the constraints imposed by these two imperatives will guarantee that the operation ends in either early termination or compromise.

Due to the nature and vulnerabilities of a surveillance operation, mirroring is the most readily identifiable aspect for surveillance detection. At the passive surveillance detection level, transition stages can force a surveillance effort into detectable mirroring actions or other conspicuous actions to maintain contact, and restrictive terrain can assist in facilitating the isolation and detection of mirroring assets as well. To put it in terms of a mathematical formula, the first category of isolations techniques (detection of mirroring) is the constant, and the other two categories (restrictive terrain and transition stages) are variables that can be employed to exploit the imperatives of contact and mirroring.

At the more active level, the target may maneuver in a manner that makes mirroring actions by surveillance assets, if present, more pronounced and readily detectable. The occurrence of transition stages in the target's travels will have a plausible purpose, but will actually be planned and orchestrated to support either surveillance detection or antisurveillance. The target will also plan the use of restrictive terrain in a manner that enables him to exploit it against the surveillance effort in order to enhance surveillance detection, or support a break in contact with the surveillance effort for surveillance detection or antisurveillance purposes.

Isolation Techniques Concept: Contact and Mirroring

In order to be effective, a surveillance effort must employ the two basic imperatives of maintaining contact and mirroring.

This concept applies to the employment of surveillance countermeasures techniques ranging from the most basic to the most sophisticated. Again, if not for this simple concept, it would not be necessary for a surveillance effort to become vulnerable to isolation or detection in the first place. The concept of mirroring employed in conjunction with the requirement to maintain contact accounts for the large majority of the more effective surveillance detection techniques. The understanding and application of this concept applies to establishing the preconditions for antisurveillance as well.

In the most basic sense, a surveillance effort exposes itself to the possibility of detection only in order to maintain contact with the target. In fact, it is those efforts to maintain contact with the target—even when the surrounding terrain and environment do not facilitate cover and concealment—that render a surveillance effort most vulnerable to surveillance detection. It is also the surveillance effort's attempts to anticipate the target's actions in the form of mirroring that may leave it vulnerable to surveillance detection.

Although the detection of mirroring by a surveillance-conscious target can be effective in isolating possible surveillance assets, it will normally not be until the target executes an active surveillance detection measure that the target will be able to confirm surveillance. In many cases, this active measure will be a maneuver to induce an asset into mirroring in a conspicuous manner that confirms surveillance.

In [Part II](#), "Surveillance Operations Overview," we addressed mirroring as it applies to the mobile surveillance follow. In basic terms, mirroring implies that a surveillance effort will travel along the same basic route as the target and at the same basic rate of speed, or pace. In addition to the fact that mirroring presents a detectable profile, it also generally implies that a surveillance asset must maintain a steady pace with the target to maintain a comfortable and secure following distance. This pace obviously impacts the pace of any other surveillance assets involved in the follow.

This dynamic, referred to as pacing, is among the most exploitable from a surveillance countermeasures perspective. By gradually fluctuating the travel pattern by pace and positioning, the target can observe for vehicles or pedestrians that mirror the same pattern. When maneuvering aggressively through traffic, the target can observe for vehicles that are also traveling behind in an aggressive manner. Conversely, by traveling in a slow and conservative manner, the target can observe for vehicles that conform to this pattern as well.

One final aspect of mirroring as it applies to isolating potential surveillance assets is the exploitation of traffic patterns and traffic flow. In many locations, the majority of the traffic tends to flow in one primary direction based on time of day or other circumstances. Vehicular and foot city commuter traffic is the most common example, but there are many other circumstances that would dictate traffic flow, such as special events and many forms of restrictive terrain. In the appropriate locations, surveillance assets that continue to mirror the target's movements when traveling against the natural flow of traffic are readily isolated from the surrounding traffic for surveillance detection purposes. Traveling against the natural flow of traffic can also present a traffic obstacle that can be exploited for antisurveillance purposes.

Isolation Methods Concept: Transition Stages

The transition stages of a surveillance operation present observable and exploitable profiles that can result in unique vulnerabilities to surveillance countermeasures.

As addressed in [Part II](#), transition stages (or transition points) provide unique opportunities for surveillance detection. Whether it be the transition among the box and follow stages of a surveillance operation, or between vehicular and foot surveillance, the transition points are junctures in the operation that render surveillance assets vulnerable to isolation due to the actions necessary to maintain contact while in transition. At the most basic level, transition points can render a surveillance effort vulnerable to isolation based on the transitions from a static to mobile or a mobile to static posture. At the more advanced level of understanding, transition stages can be employed as decisive points to implement Chaos Theory measures for both surveillance detection and antisurveillance.

The mere understanding of how a surveillance effort establishes a hasty box during temporary stops is a vital perspective. Recall that there is a *window of vulnerability* for the surveillance effort while it maneuvers to establish a hasty box when the target stops.

This also represents a surveillance countermeasures *window of opportunity* for the target. In keeping with a sound understanding of The Chaos Theory of Surveillance, the target can immediately assume the offensive by stopping and then reinitiating movement before a surveillance effort would have had the opportunity to establish secure box positions. From the surveillance detection perspective, the target can then direct efforts to isolate potential surveillance assets based on an understanding of the logical box positions that surveillance assets would be expected to assume.

In particular, the transition from vehicular to foot surveillance enables the isolation of potential assets and provides a number of possible surveillance detection options as discussed in [Part II](#) ("Transition Stages—Vehicle to Foot" and "Open Terrain"). Again, the risk to surveillance detection by foot is a general lack of protection and a limited ability to rapidly evade (accelerate away from) danger. While not always applicable to high risk threats, the transitions among vehicular and foot surveillance present a number of challenges for a surveillance effort, primarily involving vulnerabilities to isolation and "lost contact." The vulnerabilities of detection that are inherent to the Box as previously addressed are accentuated when this is coupled with the difficulties involved in the transition from a foot to a vehicular surveillance.

Isolation Methods Concept: Restrictive Terrain

The exploitation of restrictive terrain is an effective means of isolating a surveillance effort for surveillance countermeasures purposes.

Again, restrictive terrain serves primarily to isolate the surveillance effort by forcing assets into areas that restrict freedom of movement or negate cover and concealment. Methods that lead surveillance assets into restrictive terrain are common methods of isolation. Some specific applications of restrictive terrain were discussed in detail in [Part II](#).

Given the requirement to maintain contact with the target, restrictive terrain will usually force the surveillance effort to assume additional risk of detection in order to ensure that observation of the target is maintained. Surveillance vehicles may tend to close their following distance when approaching traffic hazards or obstacles such as highway interchanges or busy intersections in order to maintain observation through the obstacle. After passing the hazard, surveillance assets will tend to return to a more discreet following distance. This tendency to push in, coupled with mirroring, serves to isolate possible surveillance assets.

Open terrain is exploited to negate cover and concealment, which in turn negates freedom of movement and serves to isolate surveillance assets for detection. Open terrain forces a surveillance effort to make a trade-off between line-of-sight observation and how closely it chooses to maintain contact with the target. When the surveillance effort chooses close contact over distance, it makes itself immediately vulnerable to detection. The term “open terrain” as it applies to foot surveillance can also include areas that negate cover, not necessarily by forcing operators into the open, but by forcing them into areas where they are denied a plausible “cover for action” and therefore stand out.

Any terrain or obstacle that serves to canalize, condense, or otherwise restrict a surveillance effort can be effective in isolating assets. The most basic and common tactical employment is the “logical 180-degree turn.” This tactic is most effectively employed for surveillance detection purposes when the target has isolated potential surveillance assets in terrain that restricts their options to react in a natural and plausible manner when the maneuver is executed.

Having been isolated with limited options to react, surveillance assets will be forced to pass by the target head-on or—better yet from the surveillance detection perspective—be compelled to make a hasty and conspicuous effort to *avoid* a head-on confrontation, which serves to virtually confirm surveillance.

As a caution, although *traffic obstacles* can support surveillance detection and antisurveillance, there are risks involved that must be considered. The use of traffic obstacles, such as dense city traffic or other congested areas such as road construction sites, exploit the fact that a following surveillance effort will be hindered in its movement by the obstacles.

The same constraints or restrictions that apply to the surveillance effort, however, will also apply to the target when traveling through the obstacles. For this reason, it is important to ensure that by using these techniques, the target is not traveling into a situation that could restrict his escape options and make him more vulnerable to attack. The employment of intrusion points to draw potential surveillance assets into close proximity with the target for isolation and exploitation purposes presents

the greatest risks in this regard. These are particularly important considerations if the surveillance countermeasures employed may force the surveillance effort into a “fight-or-flight response” situation.

The Break in Contact

The break in contact is a key enabling element for both surveillance detection and antisurveillance procedures. Since it does involve the execution of multiple techniques, it is a procedure in and of itself, but as we will see in Part V, it is best employed as a key stage in the most comprehensive and effective surveillance countermeasures procedures.

As will be addressed in Part V (“The Temporary Break in Contact Surveillance Detection Procedure”), the purpose of effecting a break in contact for surveillance detection is to consciously allow surveillance assets, if present, to reestablish contact in a manner that isolates them for detection. Also in Part V (“The Break and Disappear Antisurveillance Procedure”), we will see that the primary purpose of effecting a break in contact for antisurveillance is to facilitate the subsequent execution of maneuvers to confound a potential surveillance effort’s attempts to reestablish contact. In either case, the break in contact is executed in order to manipulate the surveillance effort based on an understanding of how it thinks and reacts.

Just as the term “break in contact” implies a loss of observation by the surveillance effort, it must be executed in a manner and location that enables the target to execute follow-on maneuvers that the surveillance effort cannot observe. The employment of a “blind spot” is most germane to this concept and will be addressed in Part V (“The Temporary Break in Contact Surveillance Detection Procedure”). For antisurveillance purposes, an immediate period of “lost contact” is necessary to conduct follow-on maneuvers to confound attempts by the surveillance effort to regain contact.

Whether the objective is surveillance detection or antisurveillance, the methods employed to effect a break in contact are basically the same. The primary difference between the two is the location and circumstances under which the break in contact will be executed. The options for overt maneuvers to break contact are plentiful, but as previously discussed, these can be counterproductive if the surveillance effort perceives the activity as blatant surveillance countermeasures. If executed properly, a break in contact establishes the preconditions for effective surveillance countermeasures, based on the objectives.

The key point to understand is that the break in contact is most effectively employed as an integral stage of either a surveillance detection or antisurveillance procedure. Therefore, since it is a stage in a process, and not a means to an end in and of itself, it can be employed in a more subtle and inconspicuous manner if properly executed. The key components that facilitate effective break-in-contact efforts are pacing, acceleration, transition stages, and restrictive terrain.

Pacing

An advanced understanding and application of pacing applies to its use as a method of manipulation to generate momentum on the part of surveillance assets that can be exploited against them. A large part of a break in contact can be summarized succinctly as *using the surveillance effort’s momentum against it*. Since the surveillance effort, or individual assets thereof, will accelerate and decelerate at a pace

that is generally consistent with that of the target, the target is in essence dictating the pace of the surveillance effort. Although this concept may seem obvious, the effect is that this enables the target to control the tempo of the surveillance effort and, when appropriate, exploit the tempo against it.

In other words, the target can induce surveillance assets to either accelerate or decelerate, and then use that momentum against them for surveillance countermeasures purposes. By manipulating or controlling the pace or tempo of the surveillance effort, the target can slow the pace to generate “negative momentum” to establish the preconditions for a break in contact. The application of pacing coupled with open terrain can establish among the most suitable conditions to effect a break in contact.

Acceleration

In many cases, acceleration is a key component of any procedure involving a break in contact. In fact, many basic efforts to break contact with a surveillance effort can be categorized as “accelerate and escape.” This is another excellent example of how techniques used in isolation—rather than as part of a process—are less effective and in some cases counterproductive, depending on the surveillance countermeasures objectives. Employing a strategy of acceleration alone as a means to escape or break contact will likely be perceived as a surveillance countermeasure and will therefore be less effective than measures combining multiple aspects. By combining actions that might be characterized as “accelerate and escape” with other enabling measures, the end result is a more effective and discreet surveillance countermeasures effort.

The pacing discussion above reflects how acceleration employed as a component of a process is more effective. By inducing (manipulating) surveillance assets into “negative momentum” and then using acceleration (ideally in conjunction with other components), the target can break contact while also convincing the surveillance effort that the reason for the lost contact was its own overcautiousness or poor tactical judgment. When acceleration is incorporated in a process approach, the surveillance effort will be more inclined to perceive the reason for a break in contact as a result of its own judgment regarding how to conduct the follow, and less likely to perceive it as an active surveillance countermeasures effort.

Transition Stages

Transition stages (points) provide a multitude of opportunities to break contact with the surveillance effort. A surveillance effort will rely on target pattern analysis or other methods in an effort to predict the target’s most likely or logical actions during the preparation for or reaction to transitions stages. For this reason, transition stages provide many of the best opportunities to apply The Chaos Theory of Surveillance by performing an unanticipated action in conjunction with a transition stage.

Recall that there is a *window of vulnerability* for the surveillance effort while it maneuvers to establish a hasty box when the target stops. This also represents a surveillance countermeasures *window of opportunity* for the target. This window of opportunity enables the target to go on the offensive by stopping and then reinitiating movement before a surveillance effort would have had the opportunity to establish

secure box positions. This dynamic facilitates a break in contact with a desynchronized surveillance effort.

Even a well-established box presents vulnerabilities to the surveillance effort when the target begins to transition from a static to a mobile status. When the target departs the box, surveillance assets must pull out into traffic to establish the follow. Obviously, the faster the target is moving, the more difficult it will be to establish positive contact in the follow in a timely manner. This method can be readily employed to force a break in contact in support of surveillance detection or antisurveillance. Although this method does largely employ the element of acceleration, the fact that it is coupled with a transition stage makes it more discreet and effective.

Also recall that in establishing a box, coverage of the potential routes of travel will be prioritized based on the target's most likely utilization. When the number of possible routes exceeds the number of available surveillance assets, this prioritization drives which routes will be covered by assets and which routes will not be covered.

This prioritization may be based on target pattern analysis, but will more likely be based purely on a situational assessment of the target's most logical routes of travel. Given this understanding, the target can use reverse logic to confound the surveillance effort by traveling from the box location along a route that would likely have been given a low priority for coverage.

The transition from vehicle to foot surveillance is one of the most effective situations for effecting a break in contact. In fact, the options available by foot, particularly in crowded public locations, provide many opportunities to elude a surveillance effort. The transition from foot to vehicular surveillance involves the vulnerabilities addressed as they apply to the transition from a vehicular box to a follow, coupled with the difficulties involved with this transition. An effective chaos-inducing method is for the target to execute a stop that would require the surveillance effort to transition from a vehicular to a foot status, and then force a transition back to vehicular surveillance while the surveillance effort is still in the process of executing the initial transition.

Restrictive Terrain

Although restrictive terrain is primarily exploited in support of surveillance detection as an *isolation* method in and of itself, the obstacles characterized by many types of restrictive terrain can also be exploited to effect a break in contact that will in turn support other active surveillance detection or antisurveillance measures. In fact, with a determined and aggressive surveillance effort, obstacles that physically impede movement may be the only means to facilitate evasion.

In many cases, the use of restrictive terrain to affect a break in contact is most effective when combined with the component of acceleration. The target should accelerate prior to entering restrictive terrain or traffic obstacles to increase distance from the surveillance effort, and accelerate out of the traffic obstacle when complete to further increase separation while the surveillance effort is still obstructed by the obstacle. Open terrain can also be exploited to force the surveillance effort to increase its following distance (reverse momentum), which can in turn be exploited by acceleration and evasion to achieve a break in contact. The exploitation of traffic flow

as a traffic obstacle, by traveling against the natural flow of traffic, can also facilitate “break in contact” efforts.

Surveillance

Countermeasures

Applications:
Exploitation

Introduction to Surveillance Countermeasures Procedures

The final part of this manual consists of two surveillance detection procedures and two antisurveillance procedures. It is important to note that of the procedures detailed, the surveillance detection procedure (“The Temporary Break in Contact Surveillance Detection Procedure”) and the antisurveillance procedure (“The Break and Disappear Antisurveillance Procedure”) are endorsed as the most effective surveillance countermeasures procedures available. The other surveillance detection procedure (“The Multiple Sightings Surveillance Detection Procedure”) is a common one but it also serves as a good contrast with the more progressive and effective procedures.

Two procedures can be viewed as ingenious in their simplicity, but are frequently endorsed as the most effective available. One may question why all the technical theories, principles, concepts, and techniques that have been presented in this manual lead to only one definitive procedure for surveillance detection and one definitive procedure for antisurveillance. At the most general level, the information detailed in this manual is important for any security professional or individual with surveillance countermeasures concerns.

More specifically, a procedure is a sequence of techniques executed within a process to achieve a singular objective. As such, the procedures are broad in application and can be executed employing the range of available isolation and exploitation techniques. In fact, variations of these very procedures could be executed repeatedly against the same surveillance effort, and if orchestrated properly, would repeatedly provide plausible reasons for each episode. Once again, by playing on the individual or collective psyche, and given a logically plausible explanation, a surveillance effort will tend to rationalize and perceive these episodes as unanticipated anomalies rather than surveillance countermeasures.

As a final note of introduction to Part V, the second antisurveillance procedure (“The Temporary Break in Contact Antisurveillance Procedure”) is one that most targets will choose not to employ, but it is a fitting conclusion as it truly epitomizes the edict of “reducing the hunter to the hunted.” While this section does have great instructional and anecdotal value, it is a radical departure from the rest of this manual. In light of this, it is important to note that while this manual concludes with this section, the primary emphasis of this manual is to demonstrate how the hostile surveillance can be defeated with procedures that manipulate and exploit through techniques driven by discretion, ingenuity, and sophistication, and not through procedures employing overt actions and engagement.

The Multiple Sightings Surveillance Detection Procedure

INTRODUCTION

Tactical applications for surveillance detection techniques are well documented, but there is little in the way of documenting methodical surveillance detection procedures. However, one procedure that is well understood and widely employed among security professionals is the multiple sightings surveillance detection procedure. While this procedure involves a much more sophisticated methodology than the simple execution of individual techniques in isolation, it is still a very basic process that will not satisfy the overall surveillance countermeasures objectives of most targets. The fact that this procedure is the one that is most commonly addressed demonstrates a general lack of perspective regarding the concepts addressed in this manual and their application to the comprehensive surveillance countermeasures procedures that will be address in the following two chapters.

Perhaps the most deliberate and time-consuming form of isolation is observing for indications of the same surveillance assets in multiple locations. The multiple sightings surveillance detection procedure involves efforts to isolate surveillance assets for observation, retention, and subsequent recognition. As such, the objective is for the target to essentially isolate the surveillance effort over time for exploitation through observation. This procedure for isolation and detection is feasible only when the need to confirm surveillance is not immediate and the risk of hostile action is assessed as low, and is the procedure of choice only when that target has the latitude to conduct surveillance countermeasures activities in a more passive manner over time.

Although a very common surveillance detection procedure, the multiple sightings surveillance detection procedure is very basic in application and assumes that the target will be given multiple opportunities to observe for potential surveillance assets.

In many cases, however, the target will not have the time or want to accept the risk of a deliberate and perhaps lengthy process of detecting surveillance through multiple sightings. In fact, the most progressive surveillance detection measures are those that enable the target to cut straight to the determination of whether or not a surveillance effort exists.

This procedure is introduced as the opening of the Exploitation section of this manual despite the fact that is not proactive enough to meet the requirements of most targets. Although there is some instructional value, the more interesting purpose that this discussion serves is to demonstrate a significant contrast between this most common procedure and the more proactive, decisive, and definitive surveillance detection and antisurveillance processes in the following chapters. As such, these more comprehensive procedures will underscore just how basic and conservative this widely employed procedure actually is.

THE MULTIPLE SIGHTINGS SURVEILLANCE

DETECTION PROCEDURE

In the context of *exploit* and *manipulate*, this procedure involves the repetitive execution of two basic steps:

1. Isolate (manipulate)
2. Observe (exploit)

This procedure relies heavily on the proper execution of isolation techniques, because effective isolation is necessary to facilitate the primary means of exploitation, which is observation. In many cases, this form of isolation not only focuses on potential surveillance assets, but also involves a process of elimination to reduce the number of suspected assets to be isolated. To this end, isolation surveillance detection techniques as previously addressed are employed to observe and identify the same surveillance assets (individual or vehicle) at multiple locations. Of course, the more illogical it is that the same potential asset would be observed in the vicinity of the target at two or more locations, the higher the likelihood of surveillance.

Isolation through multiple sightings may be sufficient to confirm surveillance, or the target may choose to direct an active surveillance detection maneuver at a given suspected asset to ensure that the suspicions are not a mistake or mere coincidence. In this sense, this procedure can serve as a more deliberate isolation process in support of the more decisive surveillance countermeasures procedures detailed later in this chapter.

Although this is generally considered a more time-consuming and deliberate procedure, there are applications that enable a more progressive approach. The employment of a surveillance detection route (SDR) with preplanned surveillance detection points (SDP) is the most condensed and focused application of the procedure.

SURVEILLANCE DETECTION ROUTE

A surveillance detection route (SDR) is an advanced method of surveillance detection that is performed to induce a surveillance effort into mirroring the target's broad movements in a manner that facilitates the isolation and multiple sightings of surveillance assets. Whether developed graphically on a map or mentally, the SDR applies the understanding of surveillance detection concepts and principles to specifically planned maneuvers along a given route.

In most cases, an SDR will incorporate active surveillance detection maneuvers throughout that are executed in locations that maximize the observation of surrounding traffic at their points of execution. The ultimate objective of an SDR is to execute sequential detection maneuvers that will initially identify potential surveillance assets and subsequently isolate those assets to confirm a surveillance presence.

The most effective yet complex form of SDR is one that incorporates a theme to make an otherwise illogical route of travel appear logical. Common themes involve traveling to numerous stores as though pricing a particular item. Another effective theme is to plan an SDR around properties listed in the paper and use the guise of property hunting as a logical reason for an otherwise illogical route of travel. The

theme stop locations represent the surveillance detection points (SDPs) where the target will observe (exploit) for potential surveillance assets. Additionally, restrictive terrain and transition points along the SDR can serve as SDPs.

One of the more basic SDR applications is the “three sides of a box” technique. This concept is applicable in many situations, and does not need to be executed in a linear fashion as the name implies. The concept behind this technique is that the target will travel from one point to another by *not* taking the most direct and logical route. A very basic “three sides of a box” technique, such as employing it in a street block, is as much a mirroring detection technique as it is for multiple sightings, but a more elaborate “three sides of a box” technique over a larger area would be executed to facilitate multiple sightings.

[Figure 1](#) is a very simple example of this concept using a box that can portray a city block or other potential SDR area.

For illustration purposes, assume that the target, suspecting surveillance, is approaching point A from the bottom of the box. If point D is the target’s intended destination, he would turn right at point A and travel directly to point D. However, as a form of surveillance detection, the target will take an illogical route along the “three sides of the box” from point A through points B and C to reach point D. Any vehicle that is observed following the target through this indirect and illogical route is immediately identified as a possible surveillance asset.

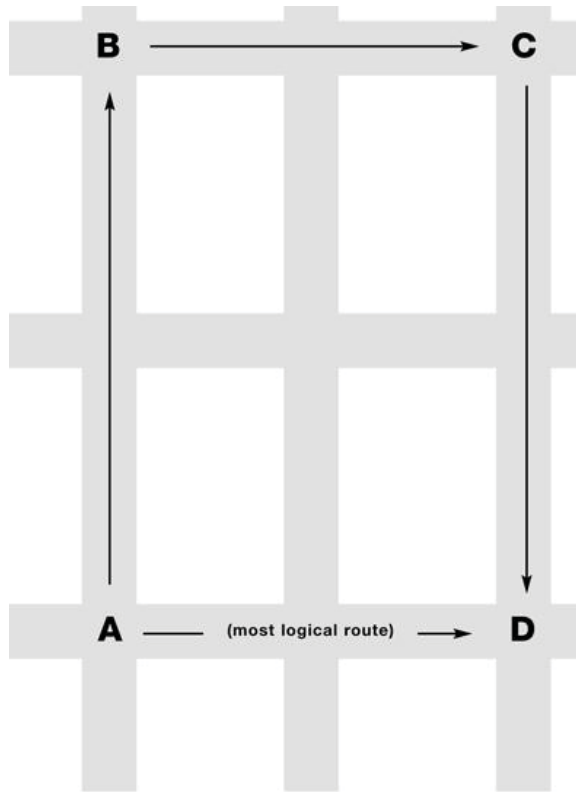


Figure 1.

Although the example in Figure 1 is the simplest possible application and may even be perceived by a surveillance effort as an overt detection maneuver, the concept is applicable in a number of variations whether the target is traveling by foot or vehicle. As such, the easier the surveillance effort is able to detect that the target is employing the method, the more likely it will be to break off prior to compromising itself. Therefore, the better planned and less discernible the technique, the more likely it will be to succeed and the less likely that it will be perceived as a detection maneuver.

In most cases, countersurveillance support (third-person surveillance detection support) will be planned and executed around an SDR with SDPs.

The Temporary Break in Contact Surveillance Detection Procedure

INTRODUCTION

Isolation can be a means to an end, but more likely will be the precursor to the execution of situation-dependent surveillance detection maneuvers. The most proactive and effective technique to facilitate isolation is the “temporary break in contact.” For surveillance detection purposes, the most effective application of the temporary break in contact is as an element of “the temporary break in contact surveillance detection procedure.” To varying degrees, all the concepts addressed to this point can be employed at some level to enable the execution of this procedure, which is invariably the most important surveillance detection weapon in the arsenal.

It is important to note that while the concepts of “contact and mirroring,” “transition stages,” and “restrictive terrain” apply directly to the isolation of potential surveillance assets, they can also be employed to enable a temporary break in contact. Even an understanding of target pattern analysis can be applied to determining when and where a surveillance effort may be most vulnerable to efforts to “break contact.”

Of particular note, the relationship between The Chaos Theory of Surveillance and the temporary break in contact surveillance detection procedure is tantamount to applying theory to practice. Recall that if not for the serious nature of a potentially hostile surveillance effort, the target could exercise elements of the Chaos Theory to “toy with” (manipulate) a surveillance effort. There is no other application that better reflects the characterization of “toy with” than the temporary break in contact surveillance detection procedure, as it can truly make the target a “master of puppets” in regard to potential surveillance assets. Like no other surveillance detection procedure, this one *manipulates* the surveillance effort in a manner that transforms it from the hunter to the hunted.

The most effective application of the temporary break in contact surveillance detection procedure consists of the target, through his actions, creating a situation in which the surveillance effort fears that it may not be able to observe the target as he passes through a traffic option. The desired response that this should elicit is that the surveillance effort reacts in an aggressive manner to avoid a “lost contact drill” situation. It is this reaction to regain contact prior to the option, in an effort to avoid a lost contact drill situation, that isolates the surveillance assets and sets the stage for this most effective application of surveillance detection.

Recall from our “Isolation Overview” discussion in [Part IV](#) that the most effective procedures to exploit the potential assets for surveillance detection purposes will employ isolation techniques to either “elicit a compromising response” or “execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response.” In the context of *manipulate* and *exploit*, the temporary break in contact surveillance detection procedure can be summarized as follows:

1. Isolate (manipulate)

2. Break in contact (manipulate)
3. Isolate (manipulate)
4. Observe (exploit)
5. Directed action (exploit) as necessary
6. Observe (exploit) if directed action is employed

THE AVOID LOST CONTACT CONCEPT

The temporary break in contact surveillance detection procedure finds its effectiveness based on the “avoid lost contact concept.” This is yet another classic example of how the seemingly complex disciplines of surveillance detection and antisurveillance can be broken down into such simple components. Just as the imperatives of contact and mirroring are extremely simple once examined, this basic cause-and-effect method of isolation for surveillance detection purposes is ingenious in its simplicity as well.

Unlike the isolation technique categories previously discussed, the avoid lost contact concept does not directly isolate surveillance assets, but it does facilitate isolation. The strength of this concept is the fact that it is based on an understanding of how a surveillance effort thinks and reacts, making it among the most effective from the surveillance detection standpoint. The concept is as follows:

When placed in a situation that risks losing contact with the target, a surveillance effort will take aggressive, and sometimes extreme measures to regain contact with the target.

The avoid lost contact concept makes the temporary break in contact surveillance detection procedure effective. Like no other concept, this is the one that truly plays on the “psyche” of a surveillance effort. Understanding that surveillance assets will react in an aggressive and potentially compromising manner to avoid a “lost contact” situation is a priceless perspective as it applies to surveillance detection.

This concept most regularly applies to the risk of losing contact with the target when approaching a traffic option. The sense of urgency that immediately besets a surveillance effort when it loses contact with the target is among the *most exploitable for surveillance countermeasures* purposes. Recall that a surveillance effort will execute a lost contact drill if the target is not observed as he reaches a traffic option or other location at which he could have taken any number of possible directions of travel. Regardless of the number of assets, for any surveillance effort the lost contact drill is a circumstance to be avoided if at all possible, because the consequences of losing contact with the target are significant. For instance, even if contact is regained during the course of the lost contact drill, a surveillance effort with multiple assets will become dispersed and will be at a disadvantage until it is able to reconsolidate the effort.

The concept of “avoid lost contact” is a significant element of the mastery of surveillance detection tradecraft. This level of insight enables the target to essentially assume control of a situation by simply exploiting the psychological impact that individual instances of lost contact have on a surveillance effort. From the team (peer) perspective, an individual surveillance operator who is responsible for allowing a lost contact situation that results in a lost contact drill has essentially failed himself and his team. The psychological motivation to avoid this fate alone generates the “inertia” and “momentum” that drive surveillance assets into positions of isolation within the

target's range of observation. Even a surveillance effort involving only one operator shares this psychological impact of the desire to avoid failure.

Regardless of the size of the surveillance effort, the motivation not to lose contact with the target is most directly related to overall mission objectives and the need to maintain contact versus the other considerations, such as vulnerability to compromise. In other words, if a surveillance effort is involved in a more deliberate and longterm mission, it will be less inclined to overreact to a potential lost contact situation, while an effort with a more immediate short-term objective will be more aggressive in ensuring that contact is maintained. Of course, while the latter is more susceptible to manipulation and isolation, it is likely a greater immediate threat to the target as well.

TEMPORARY BREAK IN CONTACT SURVEILLANCE DETECTION PROCEDURE

The "temporary break in contact" is perhaps the most effective means of isolating surveillance assets, and in many cases, is a means to the end of confirming a surveillance presence. It is important to understand that this measure does not directly involve a surveillance effort's execution of a lost contact drill. Rather, it exploits a surveillance effort's professional instincts, which are to *avoid* a lost contact situation whenever possible. In fact, it is the surveillance effort's reaction to the possibility of losing contact with the target that renders it most vulnerable to active surveillance detection. As previously noted, anytime there is a break in contact (observation) with the target, there is a sense of urgency to regain contact in a timely manner and prior to reaching a traffic option. Immediately upon a break in contact, the surveillance effort will tend to accelerate in an effort to regain contact. This tendency essentially generates a degree of "momentum" among surveillance assets that is employed against them.

The age-old tactic of turning a "blind corner" and then waiting for the surprised surveillance asset to find himself face to face with the target is a classic example of a temporary break in contact that is as ageless as intrigue and espionage. Although it can be perceived as an overt surveillance countermeasures method if not properly executed, this basic tactical application is among the very most effective surveillance detection methods, and also serves as a good example of the elements of a temporary break in contact surveillance detection procedure. These elements are:

1. Isolate in preparation for a break in contact (manipulate).
2. Effect a break in contact (manipulate).
3. Find a "blind spot" and isolate the surveillance assets when they appear and regain contact (manipulate).
4. Observe for compromising actions (exploit).
5. Execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response (exploit as necessary).
6. Observe for compromising actions (exploit) if surveillance detection maneuvers executed.

Given an understanding of the dynamics of surveillance involved, the temporary break in contact surveillance detection procedure is simple. The target will break

contact in order to orchestrate a lost contact situation that induces surveillance assets to react by accelerating to regain contact. While out of sight (“blind spot”) of the potential surveillance assets, the target will then establish, or reestablish, a rate of travel (or stop altogether) that will enable the surveillance assets to regain contact, but in a manner that enables the target to isolate the surveillance assets based on the fact that they bear down on him in an unnatural manner. In such a circumstance, surveillance assets may further isolate themselves for detection by visibly decreasing speed once they have regained contact. In fact, the best planned temporary break in contact maneuvers will be executed in a manner in which the target finds a blind spot that does not allow following surveillance assets observation of the target until they are virtually on top of him. The desired effect is that when the surveillance asset does catch up to the target, its momentum either forces it to pass by the target in a more natural manner or to decelerate in a conspicuous and detectable manner. When placed in a situation in which an immediate decision is required, many surveillance assets will “freeze” and act conspicuously (the “friction” factor). Ideally, given the appropriate restrictive terrain, the surveillance assets’ freedom of movement can be limited in a manner that gives them no option but to bear down on the target and decelerate in a conspicuous manner.

THE “BLIND SPOT”

For perspective, the time elapsed between the break in contact and the isolation of potential surveillance assets in the temporary break in contact surveillance detection procedure is generally measured in seconds. By vehicle, the execution of this technique may be a matter of less than 10 seconds from initiation to isolation and detection. Obviously, the time involved will depend on the terrain and rate of speed, but this perspective is important to the understanding that the blind spot is more of an expedient than an elaborate set of circumstances. In fact, once the target enters the blind spot, it will induce an immediate reaction from surveillance assets if the procedure is properly executed. For this reason, the blind spot can be characterized as any location or situation that causes a shortterm loss in contact (observation) that requires movement or action by surveillance assets in order to reestablish contact.

The “blind corner” is a good example for illustration purposes, but tactics and applications based on the same concepts are more accurately referred to as methods that use a blind spot. This distinction is necessary, because there are many locations other than a simple corner with physical structures preventing line of sight that are suitable to create a blind spot that facilitates a temporary break in contact. Perhaps the most common example that also has “detection” applications is that of the policeman nested away with a radar gun in a blind spot where the speeders cannot see him until they are already in range with their speeds recorded.

Recall that surveillance assets will conduct hand-offs to avoid mirroring and to minimize exposure to the target. In fact, this is a standard tactic that is executed for security when the target makes a turn. In virtually all cases, however, there is a varying amount of time—normally seconds—in which no asset will have contact (observation) with the target as the hand-off is executed. This simple factor alone can facilitate any number of variations of the blind spot (“blind corner”) method.

The concept of pacing and the target’s manipulation of a surveillance effort’s tempo in conjunction with the blind spot is the most effective means of isolation in

support of this procedure. While corners may be the most common options to create a temporary break in contact and blind spot situation, there are many other options that can be exploited with equal effect, and in many cases more discreetly. In fact, suitable terrain that facilitates speed variations to manipulate and exploit the tempo or momentum of surveillance assets enables some of the most effective applications of the temporary break in contact surveillance detection procedure.

In areas where there are bends in the road that would force a following surveillance asset to lose sight of the target temporarily (a blind spot), the target can travel at a faster speed going into the blind bend, and then decrease speed when completing it. If successful, this will result in the surveillance assets pursuing quickly around the bend and then bearing down on the target as it completes the bend. This will force the surveillance asset to either decrease its speed in an unnatural manner or pass the target. A poorly disciplined surveillance asset may even decrease its speed to reestablish a secure following distance, which will be highly indicative of surveillance.

This tactic can be used with the same effect when the target travels over the crest of a hill that would temporarily blind following surveillance assets from observing the target's activities after cresting the hill. *Although the blind bend "blind spot" technique may seem intuitively simplistic, with very few exceptions, this technique (or variations thereof) is the single most effective means of surveillance detection—ingenious in its simplicity.*

Although some of the best blind spot options have been cited as examples, the possibilities are unlimited. However, for any temporary break in contact exploiting a blind spot to be effective, there must be some type of traffic option at some point within or after the blind spot that would compel following surveillance assets to accelerate in an effort to regain contact. Among the more obvious reasons, a surveillance effort uses maps to look ahead and anticipate hazards. If there is a traffic option ahead of the target, the surveillance effort will be aware of this and react accordingly in the case of a potential lost contact situation.

By foot, the blind spot options are generally more abundant than by vehicle due to less restrictive movement options, but the temporary break in contact isolation technique applications will normally take more time to orchestrate due to the slower rate of speed.

EXPLOIT

The final stage (or stages) of the temporary break in contact surveillance detection procedure is the actual surveillance detection technique that is employed against the potential surveillance effort. Recall again that the purpose of isolating surveillance assets through the temporary break in contact is to either elicit a compromising response or execute a surveillance detection maneuver (or series of maneuvers) to elicit a compromising response.

In many cases, the fact that the surveillance asset suddenly finds itself in a vulnerable position is enough to elicit a compromising reaction. This can be accomplished by simply isolating a surveillance asset in a situation where it feels compelled to react hastily to avoid detection. If isolation alone does not sufficiently compromise the potential asset, it still serves to isolate the asset in order to focus the more active, overt, or aggressive detection measures. Once surveillance assets are isolated, an immediate surveillance detection maneuver will be directed against the

suspected surveillance asset to elicit a compromising reaction and confirm it as such. This constitutes the one-two punch that will normally force even the most savvy and composed surveillance professionals to flinch in a detectable manner.

There are a wide range of possible surveillance detection maneuvers (tactics) available, and the particular maneuver employed will be selected based on the specific situation. The options for possible surveillance detection tactics are virtually infinite, with the most common being well documented in references that deal with this less sophisticated aspect of surveillance detection.

The most aggressive directed surveillance detection techniques are those that essentially force surveillance assets into a conspicuous and detectable reaction. When the target is under the protection of a security detail and this procedure is executed using more aggressive directed techniques, it may be orchestrated in a manner that gives any potential surveillance effort the impression that the target (the detail's principal) is with the detail, when in fact he is not. The fight-or-flight response has been addressed in detail. The vast majority of surveillance efforts are intended to function as covert and discreet efforts that remain undetected throughout the entire course of a given surveillance operation.

Given this, the effectiveness of the temporary break in contact surveillance detection procedure is based on the fact that the initial and natural reaction for the vast majority of surveillance assets will be to choose "flight" without any consideration given to a "fight" response. In fact, when faced with the prospect of close contact or even a potential confrontation with the target, most surveillance assets will execute "flight," regardless of how conspicuous it may be, in order to avoid such a situation. Although this direct confrontation approach must be tempered with caution, the closer a surveillance asset suddenly finds itself to the target without plausible options for cover, the more likely it becomes that a "flight" response will be forced upon that asset in a manner that will be readily detected by the target.

As it applies to Chaos Theory, the psychological aspects of fear will very often override any consideration regarding being compromised as a surveillance asset. Such aspects range from the fear of detention to the fear of physical harm. While such directed surveillance detection methods are relatively overt and aggressive, they can still be executed in a plausible manner if incorporated with some type of logical follow-through. For example, the target can act in a manner that indicates that he is moving toward a confrontation with a potential surveillance asset, but then continue the feign to a logical conclusion that falls short of, or bypasses, the surveillance asset. From the surveillance detection perspective, this approach is the one that best characterizes the concept of reducing the hunter to the hunted, but the antisurveillance procedure detailed later ("The Break and Disappear Antisurveillance Procedure") takes this concept to its extreme manifestation.

The Break and Disappear Antisurveillance Procedure

INTRODUCTION

This chapter presents a conceptbased antisurveillance methodology that is ingenious in its simplicity. Taken at face value based on the name, the break and disappear antisurveillance procedure sounds pretty simple and straightforward, but in reality and much like the temporary break in contact surveillance detection procedure, it incorporates mutually supportive concepts and techniques that combine to form a master stroke of surveillance countermeasures.

Although the surveillance detection concepts of mirroring, restrictive terrain, and transition stages were addressed primarily as they apply to isolating surveillance assets, we have previously addressed their utility as it applies to breaking contact with a surveillance effort. There is no need to repeat these methods as they apply to antisurveillance, because the general concept of breaking contact is the same. The primary difference is that, unlike efforts to temporarily break contact for surveillance detection purposes, antisurveillance efforts are intended to be complete and enduring.

Recall that all antisurveillance measures are considered active and are the most difficult to conduct discreetly because they are generally more aggressive and conspicuous. To effect a permanent break in contact based on a single tactical application, the method must be singularly effective, meaning that it would be difficult, if not impossible, to execute without being perceived as an overt antisurveillance effort. Again, the consequences of this perception can range from intensification of future surveillance efforts to the immediate transition from a surveillance effort to an active pursuit. For this reason, any technique that makes the antisurveillance effort less detectable as such is to the target's advantage.

The most effective technique to this end is the break and disappear antisurveillance procedure, which is based on an understanding of how a surveillance effort thinks and reacts. This *procedure* is a much more effective alternative to individual antisurveillance tactics that may be effective in breaking contact but are ineffective in disguising the employment of antisurveillance activities. The break and disappear enables the target to elude and evade a surveillance effort by executing the technique in a more subtle multistage approach, as opposed to a single overt maneuver. This is most effective as it involves orchestrating a plausible break in contact that is then followed by the target inexplicably and simply disappearing.

In the context of *manipulate* and *exploit*, the break and disappear antisurveillance procedure can be summarized as follows:

1. Isolate (manipulate).
2. Break in contact (manipulate).
3. Employ reverse logic (manipulate).
4. Evade (exploit).

5. Disappear (exploit).

BREAK AND DISAPPEAR ANTISURVEILLANCE PROCEDURE

The break and disappear antisurveillance procedure methodology is based largely on the following concept:

The most effective antisurveillance techniques involve breaking contact, enabled by measures that restrict the surveillance effort's freedom of movement as appropriate, and then manipulating the understanding of how a surveillance effort will attempt to regain contact after the target is lost.

Effective antisurveillance measures are generally conducted in two sequential and complementary phases. Just as the name implies, the two stages of the break and disappear antisurveillance procedure are the “break stage” and the “disappear stage.”

THE BREAK STAGE

The first stage involves the maneuver, or series of maneuvers, to break contact with the surveillance effort. This translates to the first part of the methodology, which consists of:

. . . breaking contact, enabled by measures that restrict the surveillance effort's freedom of movement as appropriate . . .

Earlier we addressed the break in contact as a key enabling element of antisurveillance. Again, the maneuvers to effect a break in contact can be enabled by the understanding and exploitation of concepts such as mirroring (pacing), transition stages, and restrictive terrain. In addition to the other applicable concepts, an understanding of The Chaos Theory of Surveillance will enable the target to expand the effectiveness of antisurveillance efforts.

THE DISAPPEAR STAGE

The second phase of the antisurveillance effort involves the actions taken to further confound and elude the surveillance effort after initial contact is broken. If the target is able to break contact and remain unobserved until reaching the first traffic option that gives him multiple possible routes of travel, then the target enters the second phase of an effective antisurveillance routine. This phase translates to the second part of the methodology, which consists of:

. . . manipulating the understanding of how a surveillance effort will attempt to regain contact after the target is lost.

This concept is based on the understanding that a surveillance effort will continue efforts to regain contact with the target after it has been broken. For this reason, it is necessary to follow any successful break in contact with immediate follow-on measures to ensure that even the most relentless surveillance efforts are unable to recover.

Once contact is broken with the surveillance effort (actual or suspected), the true “art” of the game comes into play. Again, this is the process of understanding how a surveillance effort thinks and reacts. The “lost contact reaction” concept is the guiding

factor behind this second and conclusive evasion phase of antisurveillance methodology.

The Lost Contact Reaction Concept

Effective antisurveillance measures are based on an understanding of how surveillance will react to lost contact with the target in an attempt to regain contact.

Recall that the lost contact drill is a standard surveillance technique that involves the systematic execution of a series of maneuvers to regain observation of the target (See [Part II](#)). This basically involves the immediate prioritization of the target's likely routes of travel from the traffic option or other point of lost contact. The key point here is that the surveillance assets will search for the target based on his most likely (or logical) directions of travel. Therefore, *the obvious antisurveillance approach is for the target to travel in the most unlikely (illogical) direction from the traffic option.*

Once a break in contact is established, the target will then continue with a sequential series of *illogical* travel patterns to further confound any follow-on (logic-based) searches by the surveillance effort. Once the target is confident that surveillance has been lost, he will then rapidly travel away from the area where he broke contact, because the surveillance effort will tend to conduct an intensive search of that general vicinity.

It is important to note that whenever a surveillance effort loses contact with the target, it will rarely stop attempting to regain contact until all options have been exhausted. Even in the situation when a surveillance effort breaks contact for security to avoid being isolated in a compromising situation, it is important to understand that in most cases, contact is only relinquished to avoid a single instance of compromise, but every effort will be made to attempt and regain contact after the potentially compromising situation has subsided. Anytime the target achieves a break in contact for antisurveillance purposes, it must be immediately followed by a series of evasive maneuvers conducted to confound any follow-on efforts to regain contact.

THE BREAK AND DISAPPEAR

ANTISURVEILLANCE PROCEDURE: PRACTICAL APPLICATION

[Figure 2](#) depicts a symmetric overview of city street blocks. The target orchestrates a Break in Contact intended to ensure that he remains unsighted by any potential following surveillance assets as he enters the traffic option at Point A. Assuming that his most logical route of travel would be to continue straight toward Point B and his next most logical option would be to turn right toward Point C, the target will take the least likely and logical route toward Point D. Again, the determination of prioritizing possible options is based on target pattern analysis of the target's most likely route of travel.

For example, if traveling toward Point B is the most logical route to the target's residence and target pattern analysis would indicate that the target was likely en route home when contact was lost, the surveillance effort would conduct its lost contact drill based on this assumption. In this example, Point C would be the direction of the most likely alternative route to the target's residence or may be a direction that target

pattern analysis indicates that the target may travel if he is not going directly home, for instance to stop at a store or to get gas.

Even assuming that the surveillance effort has at least three assets to cover the three possible routes of travel, the target should be able to remain unsighted when reaching Point D, because the route he is on was given the lowest priority and was not taken until the third surveillance asset reached Point A. At Point D, the target will again take the least likely and logical route, which in this case is back toward Point E. At Point E, the target should not turn back toward his original route but should continue to take traffic options that are the opposite of the direction in which it is assumed that the surveillance effort would prioritize its search. This would involve a meandering pattern that generally takes the target out of the area of lost contact, traveling in the direction of Point G.

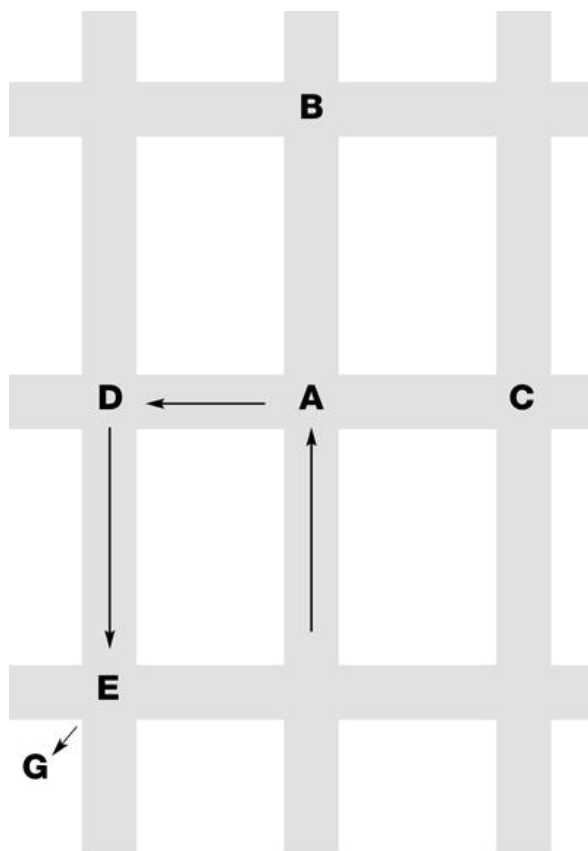


Figure 2.

For perspective, it is interesting to understand the metrics of how rapidly the break and disappear antisurveillance procedure degrades a surveillance effort’s capability. With this simple example, every option (points in the figure) through which the target

remains unsighted would require multiples of three in available surveillance assets. For instance, to conduct a minimally effective lost contact drill at the first option (Point A) the surveillance effort would require a minimum of three assets. Any fewer than this, and the target will evade surveillance without contest, again assuming that the surveillance effort searches in the target's most likely routes of travel. When the target remains unsighted at the next option, it requires that the surveillance effort have a minimum of nine surveillance assets to conduct a minimally effective lost contact drill at Point D, again assuming that Points B and C were given the priority and have six assets (three at each) dedicated to searching from those two options.

Therefore, by remaining unsighted through Point D, the target will have exhausted the capability of even the most resourceful surveillance efforts. To further make the point, by remaining unsighted through Point E, an effective lost contact drill would require 27 surveillance assets, which exceeds virtually all possible feasibilities. This example demonstrates how the number of required surveillance assets increases by multiples of three at each option—from three to nine to 27 . . .

Although a sophisticated surveillance effort with the resources to conduct a floating box is generally uncommon, the purpose of employing advanced surveillance techniques such as these is to posture for instances of lost contact as detailed in the practical application above. When the target does have reason to believe that the adversarial surveillance effort (suspected or detected) may possess such capabilities, then a variation of the break and disappear antisurveillance procedure will be executed in a location that would restrict the surveillance effort's freedom of movement to employ advanced surveillance techniques.

Accordingly, targets or security details that operate on a "worstcase" basis would plan to execute this procedure in an area with appropriate restrictive terrain as a standard practice. Among the many examples of canalized or other appropriate terrain to restrict such a capability is for the target to travel on a one-way road with the parallel routes being one-way roads in the opposite direction. The employment of this or any number of other such restrictive measures would likely require some variation to the practical application provided above, but this should require only minor adjustments based on the best available alternatives for the application of reverse logic.

The Temporary Break in Contact Antisurveillance Procedure

INTRODUCTION

A general theme throughout this manual has been the employment of intelligence and finesse to defeat a hostile intelligence threat (brains over brawn). Although this procedure employs the aspects of manipulation that make the temporary break in contact surveillance detection procedure the most effective one available, this procedure is a radical departure from the “finesse” that is characteristic of the exploit stages of the other surveillance countermeasure procedures. To this point, antisurveillance has been addressed primarily as a means to elude or evade a hostile surveillance effort. This is in keeping with the requirements and capabilities of most targets. However, there is one other element of antisurveillance that is best generically referred to as “neutralization.”

The term “neutralization” has a number of meanings, but as it applies to the temporary break in contact antisurveillance procedure, by neutralizing the surveillance effort the target renders the effort no longer capable of continuing the surveillance. This procedure is designed and intended to force decisive confrontation with the surveillance effort that will terminate the hostile surveillance threat. Potential confrontations may consist of verbal warnings by the target, or the procedure may involve the orchestration of a confrontation with law enforcement elements. Of course, more aggressive confrontations may involve shooting out the tires on surveillance vehicles, sending another type of life-threatening message to surveillance assets such as warning shots, or to the extreme, which is to neutralize the surveillance effort in the most decisive and conclusive manner. Regardless of the method of neutralization employed, this is the surveillance countermeasures procedure that definitively “reduces the hunter to the hunted.”

When this procedure is executed by a protective security detail, it will invariably be orchestrated in a manner that gives any potential surveillance effort the impression that the target (the detail’s principal) is with the detail, when in fact he is not.

THE TEMPORARY BREAK IN CONTACT

ANTISURVEILLANCE PROCEDURE: MANIPULATE

The manipulation stage of this procedure is identical to the temporary break in contact surveillance detection procedure and consists of the following three elements:

1. Isolate in preparation for a break in contact (manipulate).
2. Effect a break in contact (manipulate).

3. Find a blind spot and isolate the surveillance assets when they appear and regain contact (manipulate).

The manipulation stage of the temporary break in contact antisurveillance procedure may appear tantamount to drawing the surveillance effort into an ambush of sorts—and this is an accurate account in many ways—but this is also a very simplistic characterization of the process of getting the surveillance effort into the blind spot.

For instance, simply drawing or leading the surveillance effort into areas that restrict options for “flight” and force the “fight” does not take full advantage of the aspects of manipulation that should be available to the target or his security detail. In the context of The Chaos Theory of Surveillance, this does not leverage the aspects of inertia, momentum, friction, and general chaos that are possible.

Just as the aspects of manipulation are employed in the temporary break in contact surveillance detection procedure to achieve a degree of surprise that renders surveillance assets susceptible to detection, the same techniques of isolation and manipulation should be employed with this procedure to ensure that the surveillance effort is as surprised and poorly prepared for the confrontation as possible. Drawing an unsuspecting surveillance effort into an intrusion point is the most extreme measure of manipulation for neutralization purposes.

THE TEMPORARY BREAK IN CONTACT

ANTISURVEILLANCE PROCEDURE: EXPLOIT

This stage consists of one step:

1. Neutralize (exploit).

The target or security detail will only plan to execute a measure of neutralization that he or they are fully prepared for and capable of executing. The techniques executed in the manipulation stage of the procedure will give the target an immediate advantage over the surveillance effort’s assets, but the neutralization technique must be decisive and precise, because this advantage may only be momentary against a capable element that is prepared to rapidly assume the “fight.” As opposed to the other surveillance countermeasures procedures, the range of potential neutralization techniques is more finite, with the final in a succession of escalating options being “extreme prejudice.”

Although such applications are rare and exercised only in the most extreme circumstances, this procedure does epitomize the concept of “reducing the hunter to the hunted.” As a testament to The Chaos Theory of Surveillance, the execution of this procedure with the integration of chaos-inducing techniques is antisurveillance in its purest form, as it immediately, decisively, and without indication terminates the surveillance threat—game over, and they never saw it coming . . .

